

LINEAR SEQUENTIAL SYSTEMS OVER RESIDUE CLASS POLYNOMIAL RINGS : THEORY AND APPLICATIONS

**A Thesis Submitted
In Partial Fulfilment of the Requirements
for the Degree of
DOCTOR OF PHILOSOPHY**

**by
K. N. HARI BHAT.**

**to the
DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR
MARCH, 1985**

Dedicated to

my Parents

17 DEC 1987
CENTRAL LIBRARY

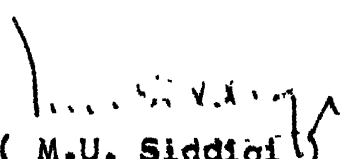
Acc. No. A 99162

EE-1985-D-BHA-LN

CERTIFICATE

Certified that this work LINEAR SEQUENTIAL SYSTEMS OVER RESIDUE CLASS POLYNOMIAL RINGS : THEORY AND APPLICATIONS by Mr. K.N. Hari Bhat has been carried out under my supervision and that this has not been submitted elsewhere for a degree.

March, 1985


(M.U. Siddiqi)
Assistant Professor
Department of Electrical Engineering
Indian Institute of Technology
Kanpur.

ACKNOWLEDGEMENTS

I wish to express my deepest sense of gratitude to my thesis supervisor, Dr. M.U. Siddiqi for his infalliable guidance and constructive criticisms. Long hours of discussions with him provided the major source of stimulation at all stages of the work.

I am thankful to Dr. V.P. Sinha for his constant encouragement and inspiring lectures which influenced me in developing an interest in Algebra and have helped me a lot in understanding the important concepts.

I am indebted to Dr. G.S. Prabhu for his continuous encouragement and valuable advice at critical moments and for extending all the facilities during the major part of stay here.

I am thankful to all my teachers here, specially Dr. S.P. Mohanty, whose lectures on Number Theory were of immense help in this work. I also wish to thank Dr. M.C. Chaudhari and Dr. K.K.S. Rathore for the helpful discussions with them, during the initial stages.

I wish to acknowledge gratefully, the authorities of Karnataka Regional Engineering College for sponsoring me for this program and IIT Kanpur for providing the financial support.

ACKNOWLEDGEMENTS

I wish to express my deepest sense of gratitude to my thesis supervisor, Dr. M.U. Siddiqi for his infalliable guidance and constructive criticisms. Long hours of discussions with him provided the major source of stimulation at all stages of the work.

I am thankful to Dr. V.P. Sinha for his constant encouragement and inspiring lectures which influenced me in developing an interest in Algebra and have helped me a lot in understanding the important concepts.

I am indebted to Dr. S.S. Prabhu for his continuous encouragement and valuable advice at critical moments and for extending all the facilities during the major part of my stay here.

I am thankful to all my teachers here, specially Dr. S.P. Mohanty, whose lectures on Number Theory were of immense help in this work. I also wish to thank Dr. M.C. Chandari and Dr. K.K.S. Kathore for the helpful discussions with them, during the initial stages.

I wish to acknowledge gratefully, the authorities of Karnataka Regional Engineering College for sponsoring me for this program and IIT Kanpur for providing the financial support.

The deepest appreciation and thanks must go to my friends, S/Shri M.G. Iswarappa, A.C. Ashok, L.S. Biradar, P.N. Sridhar, G.K. Shastri, K.V. Jayakumar, h.G. Bhandi and others, specially B.N. Shetty and P.G. Poonacha who have sacrificed a lot of time in helping me in the preparation of this thesis. I am also grateful to Sri R.K. Yaji who have helped me often in obtaining some of the relevant literatures from IIT Delhi and Dr. R.S. Shanbhag, my former teacher, for his continuous encouragement and valuable advices during his stay here.

I am thankful to Mr. J.B. Rawat and Mr. C.M. Abraham for their dedication and patience in typing the manuscript.

Finally I wish to thank my wife Shobha and children, Aparna, Bhavana and all other members of my family for their patience, tolerance and understanding which have far exceeded that normally needed in a usual family relationship.

- K.N. HARI BHAT

CONTENTS

	Page
LIST OF TABLES	xii
LIST OF FIGURES	xv
LIST OF SYMBOLS	xxi
Chapter 1 INTRODUCTION	1
1.1 Historical perspective	6
1.2 Proposed line of approach	9
1.3 Chapter outline	14
1.4 Notations and conventions	21
Chapter 2 RESIDUE CLASS RINGS OF POLYNOMIALS OVER $GF(p)$: ISOMORPHISMS, DECOMPOSITION AND ENUMERATION THEOREMS	24
2.1 Review of algebraic structures	28
2.2 Rings of polynomials over $GF(p)$	45
2.2.1 Residue class ring of polynomials over $GF(p)$ in one variable	47
2.2.2 Tensor product of rings of residue class polynomial over $GF(p)$ in one variable	53
2.3 Isomorphisms in residue class rings of polynomials	58
2.3.1 Isomorphisms in local $P_p^n[W(a)]$	63
2.3.2 Isomorphisms in $\bigcap_{i=1}^r \{P_p^{n_i}[W_i(a_i)]\}$	66
2.3.3 Isomorphisms between $P_p^n[W(a)]$ and $\bigcap_{i=1}^r \{P_p^{n_i}[W_i(a_i)]\}$	70

2.4	Decomposition of residue class rings of polynomials	79
2.4.1	Decomposition of $P_p^n[W(a)]$	80
2.4.2	Decomposition of $\times \{P_p^{n_1}[W_1(a_1)]\}$	98
2.5	Enumeration of nonisomorphic residue class rings of polynomials over $GF(p)$	101
2.6	Rings isomorphic to residue class rings of polynomials over $GF(p)$	115
2.6.1	Ring $M_p^n[W]$ of $n \times n$ matrices over $GF(p)$ isomorphic to $P_p^n[W(a)]$	116
2.6.2	Ring $\times M_p^{n_1}[W_1]$ of $n \times n$ matrices over $GF(p)$ isomorphic to $\times P_p^{n_1}[W_1(a_1)]$	129
2.6.3	Ring $Z_p^n[W]$ of n -tuples over $GF(p)$ isomorphic to $P_p^n[W(a)]$	153
2.6.4	Ring $\times Z_p^{n_1}[W_1]$ of n -tuples over $GF(p)$ isomorphic to $\times P_p^{n_1}[W_1(a_1)]$	164
3	LINEAR SEQUENTIAL SYSTEMS OVER RESIDUE CLASS RINGS OF POLYNOMIALS OVER $GF(p)$	179
3.1	State space description of LSS over residue class rings $P_p^n[W(a)]$ of polynomials over $GF(p)$	183
3.1.1	Implementation of $P_p^n[W(a)]$ -LSS	187
3.2	Response of $P_p^n[W(a)]$ -LSS	202
3.2.1	Response of periodic inputs	205
3.3	Classification and decomposition of $P_p^n[W(a)]$ -LSS	214
3.3.1	Nonsingular, singular and Nilpotent $P_p^n[W(a)]$ -LSS	214
3.3.2	Periodicity properties of characteristic matrix A	230
3.3.3	Decomposition of $P_p^n[W(a)]$ -LSS	254

3.4	LSS over other families of finite commutative rings	263
3.4.1	LSS over tensor product $\bigotimes_{i=1}^T P_p^{n_i}[W_i(a_i)]$ of residue class polynomial rings	266
3.4.2	LSS over ring $M_p^n[W]$ of $n \times n$ commutative matrices	268
3.4.3	LSS over tensor product $\bigotimes_{i=1}^T M_p^{n_i}[W_i]$ of commutative ring of matrices	273
3.4.4	LSS over ring $Z_p^n[W]$ of n -tuples	275
3.4.5	LSS over tensor product $\bigotimes_{i=1}^T Z_p^{n_i}[W_i]$ of ring of n -tuples	281
3.5	Implementation of LSS over ring of n -tuples isomorphic to the LSS over residue class polynomial rings	289
3.5.1	Implementation of LSS over $Z_p^n[W]$, $Z_p^n[W]$ -LSS	290
3.5.2	Implementation of LSS over $\bigotimes_{i=1}^T Z_p^{n_i}[W_i]$, $\bigotimes_{i=1}^T Z_p^{n_i}[W_i]$ -LSS	296
3.5.3	Implementation of $Z_p^n[W]$ -LSS isomorphic to $P_p^n[a^n-1]$ -LSS with serial multiplication	301
3.6	Isomorphism in LSS over residue class ring of polynomials over $GF(p)$	322
3.6.1	Distinct classes of $P_p^n[W(a)]$ -LSS	329
Chapter 4	AUTONOMOUS RESPONSE OF $P_p^n[W(a)]$ -LSS	332
4.1	Autonomous state response of $P_p^n[W(a)]$ -LSS	335
4.1.1	State diagram of autonomous LSS	336
4.1.2	General properties of state diagram and state response	344
4.1.3	Module structure of state response	357
4.1.4	Bounds on number of state cycles and maximum length state sequences of non-singular $P_p^n[W(a)]$ -LSS	360
4.1.5	State isomorphisms	373

4.2 Cycle length decomposition of nonsingular $P_p^n[W(a)]$ -LSS	377
4.2.1 LSS over primary $P_p^n[W(a)]$ rings	381
4.2.2 LSS over direct sum of primary $P_p^n[W(a)]$ rings	395
4.3 Autonomous response of $P_p^n[W(a)]$ -LSS	416
4.3.1 Autonomous response of canonical $P_p^n[W(a)]$ -LSS, linear recursion relations and linear recursion sequences	425
4.3.2 Generating functions of linear recursion sequences over $P_p^n[W(a)]$	433
4.4 Hamming correlation properties of sequences generated by autonomous $P_p^n[W(a)]$ -LSS	446
4.4.1 Hamming correlation functions	451
4.4.2 Bounds on values of Hamming correlation functions	458
4.4.3 Hamming correlation functions of sequences over orthogonal ideals of the same order in semisimple $P_p^n[W(a)]$ rings	476
4.4.4 Hamming correlation properties and Hamming weight structures of sequences generated by second order LSS over semisimple $P_p^n[W(a)]$ rings	479
4.5 Set of orthogonal sequences over orthogonal ideals $P_p^n[W(a)]$	488
4.5.1 Generation of orthogonal sequences	492
4.5.2 Decomposition of sequences	498
4.5.3 Transformation of sequence over primary ring into orthogonal sequences	503
4.6 Modulation and multiplexing application of sequences over orthogonal ideals	518

Chapter 5	APPLICATION TO ERROR CONTROL CODING	542
5.1	Coding problem	545
5.2	Linear block codes over $P_p^n[W(a)]$	549
5.2.1	Minimum distance and error detecting/ correcting capability	554
5.2.2	Error detection and correction	565
5.3	Linear polynomial codes over $P_p^n[W(a)]$	577
5.3.1	Generating polynomial, generator matrix and encoding principles	577
5.3.2	Minimum distance properties	605
5.3.3	Decoding principles	609
5.4	Linear cyclic codes over $P_p^n[W(a)]$	614
5.4.1	Generating polynomial, generator matrix and encoding principles	614
5.4.2	Minimum distance properties	630
5.4.3	Decoding principles	636
5.5	Encoders for polynomial and cyclic codes over $P_p^n[W(a)]$	648
5.5.1	Basic encoder structures	648
5.5.2	Encoders for interleaved polynomial and cyclic codes	666
5.5.3	Serial encoders for polynomial and cyclic codes over $P_p^n[a^n-1]$	679
5.5.4	Serial interleaved encoders	687
5.6	Decoders for polynomial and cyclic codes over $P_p^n[W(a)]$	694
5.6.1	Decoders based on polynomial division	694
5.6.2	Permutation decoder for systematic cyclic codes	701
5.6.3	Decoder based on Hamming cross- correlation properties of cyclic codes	701
Chapter 6	CONCLUSION	706
6.1	Summary of results	707
6.2	Suggestions for further work	712

APPENDICES

A	Number of irreducible polynomials of a given degree over finite field of order q	716
B	Mixed radix number system	718
C	Properties of Kronecker product of matrices	720
D	Procedure for determination of elementary divisors of matrices and computation of period of polynomials over finite fields	723
E	Chinese remainder theorem	729
F	Number of units in $\mathbb{F}_p^n[J(a)]$	731
G	Polynomial codes over $\text{GF}(p^n)$	732
H	Comparison of $\mathbb{F}_p^n[J(a)]$ and \mathbb{Z}_m	733
References		736

LIST OF TABLES

Table		Page
1.2.1	Types of residue class polynomial rings	10
2.2.1	Classification of $P_p^n[W(a)]$	50
3.2.1	Input, state and output response of $P_2^2[a^2+1]$ -LSS of Example 3.2.1	209
3.2.2a	Input, state and output of LSS of Example 3.2.2	212
3.2.2b	Input, state and output of LSS of Example 3.2.2	213
4.1.1	Nature of state cycles and state response	346
4.1.2a	Sequence of states of $P_2^2[a^2+1]$ -LSS of Example 4.1.11	375
4.1.2b	Sequence of Z_2^2 -LSS of Example 4.1.11	376
4.2.1a	State sequences of $P_2^2[a^2+a+1]$ -LSS of Example 4.2.1	385
4.2.1b	State sequences of $GF(2)$ -LSS $\simeq P_2^2[a^2+a+1]$ -LSS of Example 4.2.1	385
4.2.2a	State sequences of $P_2^2[a^2+a+1]$ -LSS of Example 4.2.2	387
4.2.2b	State sequences of $GF(2)$ -LSS $\simeq P_2^2[a^2+a+1]$ -LSS of Example 4.2.2	388
4.2.3a	State cycles of $P_2^3[a^3+1]$ -LSS of Example 4.2.6	404
4.2.3b	State cycles of Z_2^2 -LSS $\simeq P_2^3[a^3+1]$ -LSS of Example 4.2.6	405
4.3.1	Nature of autonomous response	418
4.4.1	Weight structure of sequences of Example 4.4.13	486
4.4.2	Weight structure of sequences of Example 4.4.14	488
5.2.1	$(3,1)$ linear block code over $P_2^2[a^2+1]$ and $Z_2^2 \simeq P_2^2[a^2+1]$ of Example 5.2.1	551

Table		Page
5.2.2a	Message and codewords of the $(3,1)$ single error correcting code of Example 5.2.7	569
5.2.2b	Cosets and associated syndromes of the $(3,1)$ linear block code C of Example 5.2.7	570
5.2.3a	Message and codewords of the $(3,1)$ single error detecting code of Example 5.2.8	572
5.2.3b	Cosets and associated syndromes of $(3,1)$ linear block code C of Example 5.2.8	573
5.3.1a	$u(x)$ and $y(x) = u(x) \cdot g(x)$ of Example 5.3.1	551
5.3.1b	$u(x)$ and $y(x) = u(x) \cdot g(x)$ of Example 5.3.1	552
5.3.2a	\underline{u} and \underline{y} of Example 5.3.1	583
5.3.2b	\underline{u} and \underline{y} of Example 5.3.1	584
5.3.3	Codeword polynomials of $(3,1)$ linear polynomial code of Example 5.3.3	594
5.3.4a	Message and codeword polynomials of the $(4,2)$ systematic polynomial code of Example 5.3.4	597
5.3.4b	Message and codewords of $(4,2)$ polynomial code of Example 5.3.4	598
5.3.5	Quotient $q^{(1)}(x)$ and remainder $R^{(1)}(x)$ in the division of $u(x)$ by $g(x)$	600
5.3.6	Message and codewords of the $(4,2)$ systematic polynomial code of Example 5.3.5	602
5.3.7	Message and codewords of $(4,2)$ systematic polynomial code of Example 5.3.6	604
5.3.8	Codewords of $(6,2)$ linear polynomial code of Example 5.3.7	608
5.3.9	Coset table and the associated syndromes of the $(3,1)$ polynomial code of Example 5.3.9	613

Table		Page
5.4.1a	(6,2) cyclic code of Example 5.4.2	626
5.4.1b	(6,2) systematic cyclic code of Example 5.4.2	627
5.4.2a	(6,2) cyclic code over \mathbb{Z}_2^2 , of Example 5.4.2	628
5.4.2b	(6,2) systematic cyclic code over \mathbb{Z}_2^2 of Example 5.4.2	629
5.4.4	HCCR function values between y' and $y(0), y(1), y(2), y(3)$	647

LIST OF FIGURES

Figure		Page
2.3.1	Isomorphisms between tensor product of residue class polynomial rings and residue class polynomial rings	72
3.1.1	Schematic diagram of a LSS	188
3.1.2	Basic components of $P_p^n[W(a)]$ -LSS	190
3.1.3	Implementation of LSS described by Equations (3.1.1) and (3.1.2)	191
3.1.4	Serial implementation of adder	193
3.1.5	Serial implementation of scaler $g(a)$	195
3.1.6	Scaler $(1+a^2)$ of Example 3.1.2	198
3.1.7	Scaler $(2+a)$ of Example 3.1.3	198
3.1.8	Scaler $(1+a^2+a^3)$ of Example 3.1.4	201
3.1.9	Scaler $(2+2a+a^2)$ of Example 3.1.5	201
3.2.1	$P_2^2[a^2+1]$ -LSS of Example 3.2.5	211
3.3.1a	Decomposition of $P_p^n[W(a)]$ -LSS, L (based on internal direct sum)	258
3.3.1b	Decomposition of $P_p^n[W(a)]$ -LSS, L (based on external direct sum)	258
3.3.2a	Decomposition of $P_2^3[a^3+1]$ -LSS of Example 3.2.7 (based on internal direct sum)	261
3.3.2b	Decomposition of $P_2^3[a^3+1]$ -LSS of Example 3.2.7 (based on external direct sum)	262
3.3.3a	Decomposition of $P_2^3[a^3+1]$ -LSS of Example 3.2.8 (based on internal direct sum)	264
3.3.3b	Decomposition of $P_2^3[a^3+1]$ -LSS of Example 3.2.8 (based on external direct sum)	264

Figure		Page
3.5.1	A single input single output LSS over $P_p^n[W(a)]$	290
3.5.2	A n-input n-output system over $GF(p)$	292
3.5.3a	LSS over $P_p^n[W(a)]$	293
3.5.3b	LSS over $Z_p^n \cong P_p^n[W(a)]$	293
3.5.4	Basic components of L and L'	295
3.5.5a	$P_2^2[a^2+1]$ -LSS, L of Example 3.5.1	297
3.5.5b	$Z_2^2[W]$ -LSS \cong $P_2^2[a^2+1]$ -LSS, L' of Example 3.5.1	297
3.5.6a	$P_2^2[a_1^2+1] \otimes^T P_2^2[a_0^2+a_0+1]$ -LSS of Example 3.5.2	300
3.5.6b	$Z_2^2[W_1] \otimes^T Z_2^2[W_0]$ -LSS of Example 3.5.2	300
3.5.7	Serial implementation of multiplications in $Z_p^n \cong P_p^n[a^n-1]$	303
3.5.8	Output of the serial multiplier after successive cyclic shifts	305
3.5.9	Output of the serial multiplier after successive cyclic shifts	307
3.5.10	$P_2^2[a^n-1]$ -LSS of Example 3.5.5	308
3.5.11	$Z_2^n[W]$ -LSS of Example 3.5.5	308
3.5.12	$Z_2^3[W]$ -LSS of Example 3.5.5	308
3.5.13	Serial implementation of $Z_2^n[W]$ -LSS of Example 3.5.6	312
3.5.14	Serial implementation of $Z_2^3[W]$ -LSS of Example 3.5.6	312
3.5.15a	$P_2^2[a^2+a+1]$ -LSS of Example 3.5.7	315
3.5.15b	$Z_2^2[W]$ -LSS of Example 3.5.7	315
3.5.16a	$P_2^2[a^2+a+1]$ -LSS of Example 3.5.8	318
3.5.16b	$Z_2^2[W]$ -LSS of Example 3.5.8	318

Figure		Page
3.5.17a	$P_2^3[a^3+a+1]$ -LSS of Example 3.5.9	320
3.5.17b	$Z_2^3[W]$ -LSS of Example 3.5.9	320
4.1.1	State diagram of LSS of Example 4.1.1	340
4.1.2	State diagram of LSS of Example 4.1.2	340
4.1.3	State diagram of LSS of Example 4.1.3	343
4.1.4	State diagram of LSS of Example 4.1.4	343
4.1.5a	State diagram with initial state $\begin{bmatrix} 1+a \\ 0 \end{bmatrix}$	356
4.1.5b	State diagram with initial state $\begin{bmatrix} a \\ a \end{bmatrix}$	356
4.1.5c	State diagram with initial state $\begin{bmatrix} 1 \\ a \end{bmatrix}$	356
4.5.1a	Generation of sequence $Z^{(1)}$ of Example 4.5.2	497
4.5.1b	Generation of sequence $Z^{(2)}$ of Example 4.5.2	497
4.5.2	Decomposition of sequence Z over semilocal $F_p^n[W(a)]$	501
4.5.3a	Generation of sequence Z of Example 4.5.3	501
4.5.3b	Decomposition of sequence Z of Example 4.5.3	501
4.5.4	Isomorphism between local rings and orthogonal ideals	505
4.5.5	Transformation of sequence z into orthogonal sequences $Z^{(1)}$ and $Z^{(2)}$	512
4.5.6a	Decomposition of sequence z over $F_2^4[a^4+a^2+a]$ of Example 4.5.5	512
4.5.6b	Transformation of sequences $Z^{(1)}$ and $Z^{(2)}$ of Example 4.5.5	512
4.5.6c	Generation of sequence Z over $F_2^4[a^4+a^2+a]$	512
4.5.7a	Generation of sequence Z of Example 4.5.6	517
4.5.7b	Transformation of sequence Z into orthogonal sequences $Z^{(1)}$ and $Z^{(2)}$	517

Figure		Page
4.6.1a	Modulation and multiplexing scheme	522
4.6.1b	Demultiplexing and demodulation scheme	522
4.6.2a	Alternative scheme of modulation and multiplexing	525
4.6.2b	Alternative scheme of demodulation and demultiplexing	525
4.6.3a	Modulation and multiplexing scheme of system of Example 4.6.1	530
4.6.3b	Demultiplexing and demodulation scheme of system of Example 4.6.1	532
4.6.4a	Alternative modulation and multiplexing scheme of system of Example 4.6.1	534
4.6.4b	Demultiplexing and demodulation scheme of system of Example 4.6.1	535
5.4.1	LSS of Example 5.4.4	640
5.4.2a,b,c	Typical HACR and HCCR functions	644
5.4.3a,b,c	Typical HACR and HCCR functions	644
5.5.1a	Encoder No.1 Case (i)	652
5.5.1b	Encoder No.1 Case (ii)	652
5.5.2a	Encoder No.1 over $P_2^2[a^2+1]$ of Example 5.5.1	653
5.5.2b	Encoder No.1 over $Z_2^2 \simeq P_2^2[a^2+1]$ of Example 5.5.1	653
5.5.3	Encoder No.2 based on g_r a unit	655
5.5.4	Encoder No.2 based on g_o a unit	657
5.5.5a	Encoder No.2 over $P_2^2[a^2+1]$ of Example 5.5.2	659
5.5.5b	Encoder No.2 over $Z_2^2 \simeq P_2^2[a^2+1]$ of Example 5.5.2	659
5.5.6a	Encoder No.2 over $P_2^2[a^2+1]$ of Example 5.5.3	661
5.5.6b	Encoder No.2 over $Z_2^2 \simeq P_2^2[a^2+1]$ of Example 5.5.3	661
5.5.7	Encoder No.3	662

Figure		Page
5.5.8a	Encoder No.3 over $F_2^2[a^2+1]$ of Example 5.5.4	664
5.5.8b	Encoder No.3 over $Z_2^2 \simeq F_2^2[a^2+1]$ of Example 5.5.4	644
5.5.9	Transmission of interleaved code	667
5.5.10	Interleaved Encoder No. 1	669
5.5.11	Interleaved Encoder No. 1 of Example 5.5.5	671
5.5.12	Interleaved Encoder No.2	673
5.5.13	Interleaved Encoder No.2	675
5.5.14	Interleaved Encoder No.3	676
5.5.15a	Interleaved Encoder No.3 over $F_2^2[a^2+1]$ of Example 5.5.4	678
5.5.15b	Interleaved Encoder No.3 over $Z_2^2 \simeq F_2^2[a^2+1]$ of Example 5.5.4	678
5.5.16	Serial Encoder No.1	681
5.5.17	Serial Encoder No.2	683
5.5.18	Serial Encoder No.3	686
5.5.19	Serial interleaved Encoder No.1	688
5.5.20	Serial interleaved Encoder No.2	690
5.5.21	Serial interleaved Encoder No.3	692
5.5.22a	Encoder No.3 of Example 5.5.7	695
5.5.22b	Serial Encoder No.3 of Example 5.5.7	695
5.5.22c	Serial interleaved Encoder No.3 of Example 5.5.7	695

Figure		Page
5.6.1	LSS for polynomial division: based on g_o a unit	697
5.6.2	Modified LSS for polynomial division	697
5.6.3	Serial implementation of polynomial division	699
5.6.4	LSS for polynomial division based on g_r a unit	700
5.6.5	Schematic diagram of permutation decoder	702
5.6.6a	Hamming cross-correlation decoder	703
5.6.6b	Correlator and detector of Hamming cross-correlation decoder	703

LIST OF SYMBOLS AND NOTATIONS

Σ	alphabet over which the linear sequential system is defined, or summation or cycle length decomposition
\cong	isomorphic to
$\#$	one-to-one correspondence
\forall	quantifier, for all respectively for every
\Rightarrow	implication
\triangleq	by definition
$ $	divides ; $a b$ means a divides b
\nmid	does not divide, $a \nmid b$ means a does not divide b
iff	if and only if
(m,n)	gcd of m and n
\in	quantifier belongs to or an element of $r \in R$, means r is an element of R
λ	depth of interleaving
ν	number of components in the decomposition of $P_p^n[W(a)]$
G	group or generating matrix of a code
H	subgroup of G or parity check matrix of a code
$GF(p^n)$	finite field of order p^n
R	ring
J	ideal in ring R or period of input sequence
J_p	prime ideal in R
J_m	maximal ideal in R
J_N	nilradical of R
R/J	residue class ring or quotient ring modulo J (with respect to J)

- Z_m residue class ring of integers modulo m
 $Z_p = GF(p)$, p a prime
- $e_i(a)$; orthogonal idempotent in R
- J_i ideal generated by orthogonal idempotent, $e_i(a)$
- $R \simeq R_1 \oplus R_2 \oplus \dots \oplus R$ external direct sum decomposition of R
- $R = J_1 + J_2 + \dots + J$ internal direct sum decomposition of R
- $GF(p)[x]$ ring of polynomials over $GF(p)$
- $\langle W(x) \rangle$ principal ideal generated by $W(x)$ in $GF(p)[x]$
- $\frac{GF(p)[x]}{\langle W(x) \rangle}$ the ring of residue classes of polynomials over $GF(p)$ modulo $W(x)$
- $P_p^n[W(a)] = GF(p)[x]/\langle W(x) \rangle$ where $W(x)$ is of degree n
- $r(a), g(a), q(a)$ elements of $P_p^n[W(a)]$
- h number of proper ideals in $P_p^n[W(a)]$
- $\bigotimes_{i=0}^r \{P_p^{n_i}[W_i(a_i)]\}$ tensor product of residue class polynomial rings $P_p^{n_0}[W_0(a_0)], \dots, P_p^{n_{r-1}}[W_{r-1}(a_{r-1})]$
- $q(a_{r-1} \dots a_0); g(a_{r-1}, \dots, a_0)$ elements of $\bigotimes_{i=0}^r \{P_p^{n_i}[W_i(a)]\}$
- $Z_p^n[W]$ ring of n -tuples over $GF(p)$ isomorphic to $P_p^n[W(a)]$
- $M_p^n[W]$ ring of $n \times n$ commutative matrices over $GF(p)$, isomorphic to $P_p^n[W(a)]$
- $\bigotimes_{i=0}^r \{Z_p^{n_i}[W_i]\}$ ring of n -tuples over $GF(p)$ isomorphic to $\bigotimes_{i=0}^r \{P_p^{n_i}[W_i(a_i)]\}$
- $\bigotimes_{i=0}^r \{M_p^{n_i}[W_i]\}$ ring of $n \times n$ commutative matrices over $GF(p)$, isomorphic to $\bigotimes_{i=0}^r \{P_p^{n_i}[W_i(a_i)]\}$

LSS	abbreviation for linear sequential systems or systems
Σ -LSS	LSS over alphabet Σ
A, B, C, D	characterising matrices of $\Gamma_p^n[W(a)]$ -LSS
$\bar{A}, \bar{B}, \bar{C}, \bar{D}$	characterising matrices of $Z_p^n[W]$ -LSS
A_i	component of A over J_i in the internal direct sum decomposition of A
\tilde{A}_i	component of A over $\Gamma_p^{n_i}[W_i(a)]$ in the external direct sum decomposition of A
F	figure of merit of $\Gamma_p^n[W(a)]$ -LSS
M_m	companion matrix of $m(x)$
T	period of characteristic matrix A
T_i	pseudo period of A_i , which is the component of A over internal direct sum component of $\Gamma_p^n[W(a)]$
$F(x)$	characteristic polynomial of A
$\lambda_{i(x)}^{h_{ij}}$; $i, j=1, \dots$	elementary divisors of A
$f(x)$	characteristic polynomial of linear recurrence relation over $\Gamma_p^n[W(a)]$
$f_i(x)$	projection of $f(x)$ over i th internal direct sum component of $\Gamma_p^n[W(a)]$
$\tilde{f}_i(x)$	projection of $f(x)$ over i th external direct sum component of $\Gamma_p^n[W(a)]$
$h(x)$	feedback polynomial of LSS
$\{y\}$	infinite sequence
μ	number of distinct sequences or distinct codewords upto cyclic shifts
η_{ij_1}	number of states in state cycle of length c_1 having their first component zero

n_i	number of irreducible polynomials over $GF(p)$ of degree i , or the maximum value of the number of zeros in the set of sequences of period c_1
N	period of sequence or number of symbols in a codeword over $P_p^n[W(a)]$
K	order of LSS or number of message symbols in a codeword over $P_p^n[W(a)]$
r	number of check symbols in a codeword
d	minimum distance of code
t	time instant or error correcting capability of code
$g(x)$	generating polynomial of code
u	message word
$u(x)$	message word polynomial
y_i	codeword or finite length sequence
$y(x)$	codeword polynomial or generating polynomial of linear recurring sequence
y'	received word
$y'(x)$	received word polynomial
Z	sequence over $P_p^n[W(a)]$ or Z_p^n
$Z(i)$	sequence over i th orthogonal ideal
$H_y(\tau)$	Hamming autocorrelation function of y
$H_{yz}(\tau)$	Hamming cross-correlation function between y and z
W_y	Hamming weight of finite length sequence y
D_{yz}	Hamming distance between finite length sequences y and z of equal length
σ^i	right cyclic shift by i locations
π^i	right or left cyclic shift by i locations depending on the context

Z	sequence over $\Gamma_p^n[W(a)]$
\underline{Z}	sequence over $Z_p^n[W(a)]$
s	a solution of 2nd order linear recurrence relation over semisimple $\Gamma_p^n[W(a)]$, which is a periodic infinite sequence
s_i	maximum-length sequence over orthogonal ideal J_i isomorphic to finite field
\tilde{s}_i	s modulo $[p; W_1(a)]$ is a maximum length sequence over $\Gamma_p^{n_i}[W_1(a_i)]$
\tilde{s}_i^j	a segment of sequence s_i
y_j	j th element of sequence \tilde{s}_i^j
$+$	direct sum or addition modulo N depending on the context
\times	Kronecker product or tensor product depending on the context
W_1	companion matrix of $W_1(a)$
W_{1ij}	ij th element of W_1
\underline{W}_j	j th column of W_0

SYNOPSIS

This work introduces as a generalisation of linear sequential systems over finite fields the notion of linear sequential systems over residue class rings of polynomials over finite fields and gives theory and applications of these systems. Structural properties, implementation and analysis of such systems and their applications in error control coding and generation of sequences over residue class rings of polynomials are presented. Properties of the sequences and their applications in modulation and multiplexing of data sequences over finite fields are considered.

Study of linear sequential systems (LSS) over the finite field $GF(2)$ was initiated by Huffman, which was later generalised by several investigators to systems over $GF(p)$ and $GF(p^n)$. LSS over $GF(p^n)$ are described by input space, output space and state space, which are vector spaces of appropriate dimension over $GF(p^n)$, and characterising matrices A, B, C and D of appropriate sizes over $GF(p^n)$.

Finite field $GF(p^n)$ is a specific case of residue class ring of polynomials, denoted by $P_p^n[W(a)]$, where $W(a)$ is the modulus polynomial of degree n over $GF(p)$; $P_p^n[W(a)]$ becomes $GF(p^n)$ when $W(a)$ is irreducible. LSS over $P_p^n[W(a)]$, denoted by $P_p^n[W(a)]$ -LSS, are thus a generalisation of LSS over $GF(p^n)$.

In $P_p^n[W(a)]$ -LSS the sets of inputs, outputs and states are free modules over $P_p^n[W(a)]$ and the characterising matrices A, B, C and D are over $P_p^n[W(a)]$.

By appropriate definition of addition and multiplication operations it is possible to obtain rings of n -tuples and $n \times n$ commutative matrices over $GF(p)$, which are isomorphic to $P_p^n[W(a)]$. LSS defined over these rings of n -tuples and $n \times n$ matrices are then isomorphic to $P_p^n[W(a)]$ -LSS, which can be viewed as LSS which process n -tuples or $n \times n$ matrices from the respective rings. A $P_p^n[W(a)]$ -LSS can be implemented over $GF(p)$ using the isomorphism between $P_p^n[W(a)]$ and the ring of n -tuples.

LSS defined over tensor product of residue class polynomial rings over $GF(p)$ give rise to additional families of LSS. In this case also isomorphisms can be established between tensor product residue class polynomial rings, rings of n -tuples, and rings of $n \times n$ commutative matrices over $GF(p)$. Using these isomorphisms LSS over tensor product of residue class polynomial rings can be implemented over $GF(p)$.

In finite fields the operations of addition, subtraction, multiplication and division are all defined. However, in a ring the operation of division is not defined. As a consequence the generalisation considered in this thesis is not trivial.

It is known that finite fields of a given order are all isomorphic to each other. However, in a ring this is not true. The set of all isomorphic residue class polynomial rings of a given order p^n constitutes an equivalence class and LSS defined over these rings constitute a distinct class of LSS. Number of such distinct classes of LSS is equal to the number of non-isomorphic residue class polynomial rings of order p^n ; LSS defined over $GF(p^n)$ constitute one of these classes. Enumeration of nonisomorphic residue class polynomial rings of a given order, or equivalently of the distinct classes of LSS is carried out. It is shown that the number of nonisomorphic residue class polynomial rings of a given order p^n and hence the number of distinct classes of $P_p^n[W(a)]$ -LSS depends on the partition function of n and the number of irreducible polynomials of degree $1, 2, \dots, (n-1)$ over $GF(p)$. Since the properties of LSS depend on the ring over which it is defined, LSS over $P_p^n[W(a)]$ offer, in comparison to the conventional LSS over finite fields, a wider choice of systems.

The analysis and applications of LSS over residue class polynomial rings discussed here are based mainly on the decomposition of rings into external direct sum of primary rings or internal direct sum of ideals generated by orthogonal idempotents. LSS defined over rings can, therefore, be decomposed into component systems defined over primary rings which are either finite fields or local rings. The decomposition of

$P_p^n[W(a)]$ into primary rings gives rise to implementation of $P_p^n[W(a)]$ -LSS using subsystems over primary rings. Likewise decomposition of $P_p^n[W(a)]$ into internal direct sum of orthogonal ideals gives rise to implementation of $P_p^n[W(a)]$ -LSS using subsystems over orthogonal ideals.

In the study of the response of $P_p^n[W(a)]$ -LSS the characteristic matrix A plays a prominent role. The conditions for A to be singular, nilpotent and nonsingular are derived. It is shown that when A is singular but not nilpotent, the response is either periodic or ultimately periodic depending on the initial state. When A is nilpotent, the response is ultimately a zero sequence and when A is nonsingular the response is periodic, irrespective of initial state. It is shown further that if A is nonsingular and hence periodic with period say, T , and input is periodic with period J , then the output of $P_p^n[W(a)]$ -LSS is also periodic with a period which divides pJT .

The maximum possible period of a state cycle is equal to the period of A . If the initial state has components from an ideal then all the states in the state cycle will have components from the same ideal. The number of state cycles is thus at least equal to the number of ideals in $P_p^n[W(a)]$ over which the LSS is defined. The structure of state cycles of $P_p^n[W(a)]$ -LSS is obtained in terms of the structure of state cycles with respect to the direct sum components of the characteristic matrix A of the LSS.

Under autonomous operation the output sequence of a $P_p^n[W(a)]$ -LSS is a fixed linear transformation of the state sequence and the set of all output sequences constitutes a module. For the single output canonical system the autonomous response is a linear recursion sequence, i.e., the output sequence satisfies a linear recursion relation over $P_p^n[W(a)]$, and the set of all such sequences constitutes a free module. Hamming correlation properties of linear recursion sequences over $P_p^n[W(a)]$ are studied. Bounds on the values and number of levels of correlation functions are derived.

It is shown that sequences over orthogonal ideals generated by distinct orthogonal idempotents are pointwise orthogonal. Since an arbitrary sequence over a semisimple or semilocal ring can be decomposed into an internal direct sum of component sequences over orthogonal ideals, these component sequences are inherently pointwise orthogonal sequences. An arbitrary sequence over a finite field or a local ring can be first mapped into a sequence over an appropriate semilocal or semisimple ring and then decomposed into sequences over orthogonal ideals. Such orthogonal sequences can be used for modulating and multiplexing data sequences with elements from finite fields. For this purpose source sequences over finite fields are transformed into orthogonal sequences over orthogonal ideals in an appropriate semisimple ring. Each orthogonal sequence then modulates a maximum length sequence over

the same ideal. Modulated sequences corresponding to different sources are added and transmitted as a single multiplexed sequence over the semisimple ring. The orthogonality property of sequences over orthogonal ideals is used for separating (demultiplexing) the component sequences at the receiver. Each individual sequence is then Hamming cross-correlated with the reference sequence for demodulation.

Applications of LSS over residue class polynomial rings in the generation of nonsystematic and systematic linear polynomial and cyclic codes over $P_p^n[W(a)]$ and decoding of these codes are considered. In the polynomial and cyclic codes every codeword, expressed as a polynomial over $P_p^n[W(a)]$, is a multiple of a fixed polynomial, called generator polynomial. These codes are encoded by polynomial multiplication employing appropriate $P_p^n[W(a)]$ -LSS. An (N,K) polynomial code over $P_p^n[W(a)]$ is a free submodule of rank K and order p^{nK} . It is shown that the set of all autonomous responses of a nonsingular single output canonical $P_p^n[W(a)]$ -LSS has the structure of a linear cyclic code which is an ideal in the residue class polynomial ring modulo (x^N-1) over $P_p^n[W(a)]$. Decoding of polynomial and cyclic code is done by employing LSS which perform polynomial division. If the remainder is nonzero, error is detected. If the error is within the correcting capability the remainder is uniquely related to the error polynomial which is obtained from the decoding table and subtracted from the received polynomial. In the case of cyclic codes it is

shown that the decoding can be done by computing the Hamming cross-correlation between the received codeword and a set of reference codewords available at the receiver. The reference word which gives the maximum cross-correlation value and the shift at which this occurs are utilised for decoding the received word. For the case of systematic cyclic codes permutation decoding can be employed on the lines similar to permutation decoding of systematic cyclic codes over finite fields.

CHAPTER 1

INTRODUCTION

This work is concerned with the theory and applications of linear sequential systems (LSS) over residue class rings of polynomials over finite fields which constitute a generalisation of LSS over finite fields. Structural properties, implementation details and autonomous response of the systems are studied and their applications in encoding and decoding circuits for error control, generation of sequences and modulation and multiplexing of digital data are considered.

LSS, in general are linear shift invariant systems with elements of input and output sequences from a finite alphabet and they constitute an important subclass of finite state systems [1,2]. If the alphabet is, say Σ , then the LSS with Σ as alphabet are denoted by Σ -LSS, read as LSS over the finite alphabet Σ .

The theory of LSS for the case when the alphabet corresponds to a finite field is well established [3-17]. In an m -input and j -output LSS of order K , over finite field $GF(p^n)$ (i.e., $GF(p^n)$ -LSS), the input and output sequence elements are m -tuples and j -tuples over $GF(p^n)$. Such a system is defined by the following :

- (i) A vector space U over $GF(p^n)$ of dimension m called the input space,

- (ii) a vector space Y over $GF(p^n)$ of dimension j called the output space,
- (iii) a vector space X over $GF(p^n)$ of dimension K called the state space
- (iv) transformations which map the elements $x(N) \in X$ and $u(N) \in U$ into $x(N+1)$ and $y(N)$ given by

$$\text{Next state function : } x(N+1) = Ax(N) + Bu(N) \quad (1.1.1)$$

$$\text{Output function : } y(N) = Cx(N) + Du(N) \quad (1.1.2)$$

where N denotes integral time instants $0, 1, 2, \dots$, the matrices A, B, C and D have elements drawn from $GF(p^n)$ and are called the characterising matrices of LSS. A is specifically called the characteristic matrix of the LSS. Given an initial state $x(0)$ and an input sequence $u(0), u(1), \dots$, the corresponding sequences of states and outputs can be computed recursively from the state and output equations (1.1.1) and (1.1.2) respectively.

A $GF(p^n)$ -LSS with the characteristic matrix A in the form

$$A = \left[\begin{array}{c|ccc} 0 & & & I_{K-1} \\ \hline & & & \\ \hline a_K & & a_{K-1} & \dots & a_1 \end{array} \right]$$

where I_{K-1} is the identity matrix of order $(K-1)$, is called a canonical $GF(p^n)$ -LSS. The autonomous response of a single output, canonical $GF(p^n)$ -LSS, with $C = [1 \ 0 \ \dots \ 0]$ satisfies a linear recursion relation over $GF(p^n)$ and is called a linear

recursion sequence. When the characteristic polynomial of A is primitive over $GF(p^n)$, output sequences are periodic with period equal to $(p^{nK}-1)$, the maximum possible value; such sequences are called maximum length sequences [9-11].

$GF(p^n)$ -LSS, specifically $GF(2)$ -LSS and $GF(2^n)$ -LSS, find applications in various areas such as computing circuits [12, 13, 18, 19] encoding and decoding circuits [16-21] and sequence generators [9-11].

In this thesis we consider LSS over residue class ring of polynomials modulo a polynomial $W(a)$ of degree n , over $GF(p)$. Addition and multiplication operations in this ring are the usual polynomial addition and multiplication modulo p and modulo $W(a)$. Such a ring is a finite commutative ring of order p^n with identity. We denote these rings by $P_p^n[W(a)]$. LSS over $P_p^n[W(a)]$ are accordingly denoted by $P_p^n[W(a)]$ -LSS. They have a basic description similar to that given earlier by (1.1.1) and (1.1.2) for the case of $GF(p^n)$ -LSS; in this case the elements of input, output and state sequences are respectively m -tuples, j -tuples and K -tuples over $P_p^n[W(a)]$, which constitute free modules (over $P_p^n[W(a)]$) of rank m, j and k respectively.

Finite fields $GF(p^n)$ are a specific case of $P_p^n[W(a)]$; when $W(a)$ is irreducible over $GF(p)$, $P_p^n[W(a)]$ becomes $GF(p^n)$. $GF(p^n)$ -LSS is therefore a specific case of $P_p^n[W(a)]$ -LSS. The results given in this thesis may, therefore, be seen as a

generalisation of the results on $GF(p^n)$ -LSS.

Although the description, as given by (1.1.1) and (1.1.2), and consequently the analysis procedures of LSS over any finite alphabet, in general, remain the same, the properties and applications of such systems vary significantly depending upon the properties of the specific algebraic structure over which the systems are defined. Towards this end first of all it is noted that in a finite ring, unlike a finite field, the notion of multiplicative inverse does not exist for elements which are zero divisors. Specifically in $P_p^n[W(a)]$, elements which are factors of $W(a)$ are zero divisors and hence the multiplicative inverse of such ring elements is not defined. Next it is noted that finite fields of the same order are all isomorphic to each other, whereas all the commutative rings of the same order need not be isomorphic to each other. For example, Z_4 (the ring of residue class integers modulo 4) and $P_2^2[a^2+1]$ are not isomorphic, although both of these are commutative rings of order 4. Even all the residue class polynomial rings of the same order are not isomorphic to each other. The set of all isomorphic residue class polynomial rings of any given order constitutes an equivalence class and each equivalence class of residue class polynomial rings gives rise to a distinct class of LSS. In view of the foregoing considerations, the study of $P_p^n[W(a)]$ -LSS should not be taken as a trivial generalisation of the study of $GF(p^n)$ -LSS.

The study of $P_p^n[W(a)]$ -LSS provides a compact and generalised framework for the study of linear sequential systems which can process sequences constructed from the set of n -tuples over $GF(p)$ or $n \times n$ matrices over $GF(p)$ as explained below.

The ring $Z_p^n[W]$ of n -tuples over $GF(p)$ and the ring $M_p^n[W]$ of $n \times n$ commutative matrices over $GF(p)$, can be constructed by appropriately defining addition and multiplication operations in the set of n -tuples and $n \times n$ commutative matrices over $GF(p)$ respectively, such that both these rings are isomorphic to $P_p^n[W(a)]$. Then $Z_p^n[W]$ -LSS and $M_p^n[W]$ -LSS of order K , which process n -tuples and $n \times n$ matrices from the respective rings, can be seen as a subclass of $GF(p)$ -LSS of order nK . Because of the isomorphisms between $Z_p^n[W]$, $M_p^n[W]$ and $P_p^n[W(a)]$, such $GF(p)$ -LSS of order nK can be studied in terms of $P_p^n[W(a)]$ -LSS of order K , which reduces the complexity of analysis.

Besides the formal description of $P_p^n[W(a)]$ -LSS and expressions for state and output sequences, the following topics have received particular attention in this thesis.

- (i) Enumeration of non-isomorphic $P_p^n[W(a)]$ rings of specified order which gives various classes of non-isomorphic $P_p^n[W(a)]$ -LSS.
- (ii) Construction of rings $Z_p^n[W]$ of n -tuples and rings $M_p^n[W]$ of $n \times n$ commutative matrices over $GF(p)$, isomorphic to residue class rings of polynomials over $GF(p)$. This helps us in the implementation of $P_p^n[W(a)]$ -LSS of order K in terms of $GF(p)$ -LSS of order nK .

- (iii) Periodicity properties of characteristic matrix A , families of LSS defined over other algebraic structures isomorphic to $P_p^n[W(a)]$ and LSS over tensor product of residue class polynomial rings.
- (iv) Analysis of autonomous response of $P_p^n[W(a)]$ -LSS in general and the linear recursion sequences in particular, the latter include maximal length sequences over $P_p^n[W(a)]$.
- (v) Cyclic or periodic Hamming correlation properties of sequences over $P_p^n[W(a)]$; cyclic Hamming correlation between two sequences is defined [22] as the number of positions in which the sequences have identical symbols.
- (vi) Application of $P_p^n[W(a)]$ -LSS in the generation of sequences and encoding and decoding of polynomial and cyclic codes over $P_p^n[W(a)]$.
- (vii) Application of sequences generated by $P_p^n[W(a)]$ -LSS in modulation and multiplexing of data sequences.

1.1 HISTORICAL PERSPECTIVE

Historically, the study of LSS was initiated in the context of error correcting codes by Huffman [3] who considered LSS over binary alphabet, that is, $GF(2)$ -LSS. The notion of $GF(2)$ -LSS was then generalised to $GF(p)$ -LSS by several investigators [4-7] followed by generalisation to $GF(p^n)$ -LSS [8]. $GF(p^n)$ -LSS of order K are equivalent to $GF(p)$ -LSS of order nK . As a consequence $GF(p^n)$ -LSS are implemented and analysed as

$GF(p)$ -LSS [12,13,23,24].

The study of linear recursion sequences (LRS) over finite alphabet, as pointed out in the preface of [11], goes as far back as Lagrange in the eighteenth century. The periodicity properties of LRS over finite alphabet have been studied by Carmichael [25], Ward [26], and Hall [27] in the second quarter of the present century. In the context of LSS, LRS can be viewed as the autonomous response of a single output canonical $P_p^n[W(n)]$ -LSS. Study of binary maximal length sequences was pioneered by Zierler [10] and Golomb [11]. Majority of the applications using binary maximal length sequences are based on their periodic correlation properties [10,11,28,29], the correlation functions being defined in terms of the usual inner product of sequences [22,28,29]. Maximal length sequences have been utilised in scramblers [30,31], spread spectrum communication systems [32-34], code division multiple access systems [32-35], synchronisation systems for digital communication systems [36], communication systems for multipath channels [37], fault detection in digital systems [38] and range finding [39].

A method of constructing sequences with elements from finite fields and having optimal cyclic Hamming correlation properties has been given by Lempel and Greenberger [22] who have shown that maximal length sequences over $GF(p)$ have two level Hamming autocorrelation functions.

LSS over finite commutative ring Z_m , the ring of residue class integers modulo m , have been studied in the recent past [40-42]; the periodicity properties of the state response and the output are given in [40,41] and the operational calculus for LSS over Z_m has been developed in [43]. An exhaustive review of the work done on linear systems over commutative rings is presented by Sontag [44,45]; linear systems in this review mainly consist of linear dynamical systems over principal ideal domains [46,47], which are commutative rings without zero divisors and whose ideals are principal ideals.

Error correcting codes over finite commutative rings of integers have been investigated by Blake [48,49]. He has given a method [48] to construct linear cyclic codes over semisimple ring of integers Z_m from cyclic codes over the direct sum components of Z_m . The minimum distance of such a code is the minimum of the minimum distances of the component codes. Blake [49] has also investigated the properties of linear codes over Z_q (q = power of a prime) analogous to the familiar Hamming, Reed Solomon and BCH codes over finite fields. Spiegel [50] has investigated the codes over residue class ring Z_m for any positive m . Murakami and Reed [51] have investigated classes of codes for a multi-channel communication system. They have developed a fast algorithm to calculate syndrome of linear systematic block and convolutional codes over direct sum of Galois fields. They have shown that any set of finite state linear shift invariant sequential

circuits on Galois fields of integers can be implemented by a single finite state linear shift invariant sequential circuit on a finite ring of integers.

As far as systems over residue class polynomial rings are concerned, the scheme proposed by Rader et al [52] for the generation of random numbers is worth mentioning here. In this scheme two binary n -bit shift registers with feedback are used to generate sequences of n -tuples which are converted to decimals and the system is analysed as a $GF(2)$ -LSS of order $2n$. This scheme as we shall see in this thesis may be interpreted as a special case of $Z_p^n[W]$ -LSS isomorphic to $P_2^n[a^n-1]$ -LSS of order 2. With this interpretation core of the random number generator proposed in the above scheme may be analysed in a much simpler manner.

1.2 PROPOSED LINE OF APPROACH

The structure and properties of $P_p^n[W(a)]$ are decided by the relatively prime factors in the prime factorisation of the modulus polynomial $W(a)$. Based on the factorisation of $W(a)$, residue class polynomial rings may be classified into four categories as given in Table 1.2.1. For the case when $P_p^n[W(a)]$ is a field, study of $P_p^n[W(a)]$ -LSS of order K can be carried out either as $GF(p^n)$ -LSS of order K or as $GF(p)$ -LSS of order nK [12,13]. Study of LSS over local $P_p^n[W(a)]$ is carried out in terms of isomorphic systems over $GF(p)$. Semisimple and semi-local rings can be decomposed into external direct sum of

Table 1.2.1 Types of Residue Class Polynomial Rings

Type of $\mathcal{W}(a)$	Type of Ring	Remarks
Irreducible polynomial over $\text{GF}(p)$	Finite field	$P_p^n[\mathcal{W}(a)]$ is a primary ring isomorphic to $\text{GF}(p^n)$
Power of an irreducible polynomial over $\text{GF}(p)$	Local ring	$P_p^n[\mathcal{W}(a)]$ is a primary ring
Product of ν irreducible polynomials over $\text{GF}(p)$	Semisimple ring	$P_p^n[\mathcal{W}(a)]$ is isomorphic to external direct sum of finite fields and equal to internal direct sum of ν orthogonal ideals
Product of powers of ν irreducible polynomials over $\text{GF}(p)$	Semilocal ring	$P_p^n[\mathcal{W}(a)]$ is isomorphic to external direct sum of local rings and equal to internal direct sum of ν orthogonal ideals

primary rings or internal direct sum of ideals generated by orthogonal idempotents which are isomorphic to primary rings; the ideals generated by orthogonal idempotents have been called as orthogonal ideals. In these decompositions the role of irreducible polynomials and their powers is similar to the role of primes and prime powers in the decomposition of residue class integer ring \mathbb{Z}_m . Decompositions of $P_p^n[W(a)]$ gives rise to decompositions of $P_p^n[W(a)]$ -LSS into isomorphic systems over component primary rings or orthogonal ideals. In the case of systems over semisimple ring, each component system is over a field. In the case of systems over semilocal ring, the component systems are over local rings and finite fields.

The decomposition of $P_p^n[W(a)]$ and $P_p^n[W(a)]$ -LSS play a central role in the studies carried out in this thesis. Specifically this notion is used in the following.

- (i) Enumeration of distinct classes of LSS over residue class polynomial ring of a given order.
- (ii) Implementation of $P_p^n[W(a)]$ -LSS using subsystems over primary rings or over ideals isomorphic to primary rings.
- (iii) Computation of period of characteristic matrix A over $P_p^n[W(a)]$.
- (iv) Cycle length decomposition of states of $P_p^n[W(a)]$ -LSS.
- (v) Decomposition of sequences over $P_p^n[W(a)]$ into orthogonal sequences.

- (vi) Study of Hamming correlation property of sequences over $P_p^n[W(a)]$ and computation of minimum distance of cyclic codes over semisimple $P_p^n[W(a)]$ in particular.

Key ideas underlying the application of $P_p^n[W(a)]$ -LSS in generation of sequences and their applications and encoding and decoding are as given below.

- (i) In a semisimple or semilocal $P_p^n[W(a)]$, the ring elements belonging to distinct orthogonal ideals annihilate each other. As a consequence set of sequences over orthogonal ideals annihilate each other on a pointwise basis. We call such sequences as orthogonal sequences. If such sequences are interpreted as sequences over $Z_p^n[W]$, then the sequence elements are n -tuples over $GF(p)$. Orthogonal sequences can be generated by single output canonical $P_p^n[W(a)]$ -LSS with initial condition from an orthogonal ideal. Furthermore, any arbitrary sequence over $P_p^n[W(a)]$ can be decomposed into orthogonal sequences, where each sequence is over an orthogonal ideal. A ring $P_p^n[W(a)]$ can be embedded into an appropriate larger semilocal or semisimple ring. Thus sequences over an arbitrary $P_p^n[W(a)]$ can be transformed (embedded) into sequences over orthogonal ideals in the larger ring. These sequences can be used in modulation and multiplexing of data sequences. A sequence over an orthogonal ideal in $P_p^n[W(a)]$, which is isomorphic to maximal length sequence over an appropriate finite field, is modulated by a

data sequence. Several such sequences are added (multiplexed) modulo $[p; W(a)]$ and transmitted as a single sequence over $P_p^n[W(a)]$. At the receiver, the received sequence is demultiplexed into its component sequences, using the pointwise orthogonality property of sequences. The separated sequences are demodulated by Hamming cross \times correlation.

(ii) As pointed out earlier, there is one-to-one correspondence between the elements of residue class polynomial ring $P_p^n[W(a)]$ and the ring $Z_p^n[W]$ of n -tuples over $GF(p)$. If we consider blocks of length n in a sequence of symbols from $GF(p)$, a mapping of K such blocks into N blocks can be defined which results in an (N, K) block code over $Z_p^n[W]$. Because of isomorphism between $P_p^n[W(a)]$ and $Z_p^n[W]$, the (N, K) block codes over $Z_p^n[W]$ can be studied in terms of (N, K) block codes over $P_p^n[W(a)]$. Such a study is much more compact as there is reduction in dimension. In the specific case when $W(a)$ is irreducible over $GF(p)$, we get (N, K) block codes over $GF(p^n)$. The relevant theory of linear block codes and its specific classes, polynomial codes and cyclic codes over $P_p^n[W(a)]$ is developed in a manner similar to the theory of codes over finite fields [17-21, 53, 54]. The effect of zero divisors in the ring on the choice of parity check matrix and generating polynomial have been studied. $P_p^n[W(a)]$ -LSS may be employed to implement encoders and decoders for codes over $P_p^n[W(a)]$ on lines similar to the use of $GF(p^n)$ -LSS for encoders and decoders over finite fields.

1.3 CHAPTER OUTLINE

Necessary mathematical background for the study of LSS over residue class polynomial ring and their applications is presented in Chapter 2. This mainly includes results on residue class polynomial rings $P_p^n[W(a)]$ and tensor product of r residue class polynomial rings $P_p^{n_0}[W_0(a_0)], P_p^{n_1}[W_1(a_1)], \dots$ and $P_p^{n_{r-1}}[W_{r-1}(a_{r-1})]$, denoted by $\bigotimes_{i=0, \dots, r-1}^T \left\{ P_p^{n_i}[W_i(a_i)] \right\}$.

Depending upon the prime power factorisation of $W(a)$, $P_p^n[W(a)]$ rings are classified as finite fields, local rings, semisimple rings or semilocal rings. The results concerning isomorphisms and decomposition of semisimple or semilocal $P_p^n[W(a)]$ rings into internal direct sum of orthogonal ideals or the external direct sum of primary rings are presented as an adaptation of the results of commutative algebra.

All the residue class polynomial rings of the same order need not be isomorphic to each other. An expression for the number of nonisomorphic residue class polynomial rings of order p^n is obtained. This makes use of the results of isomorphism and decomposition of rings, number of irreducible polynomials of degree $\leq n$, and the partition and restricted partition function [55] of integers $\leq n$.

Procedures for construction of rings $Z_p^n[W]$ of n -tuples and rings $M_p^n[W]$ of $n \times n$ commutative matrices isomorphic to $P_p^n[W(a)]$,

and tensor product rings $\bigotimes^I \{Z_p^{n_i}[W_i]\}$ of n -tuples and $\bigotimes^I \{M_p^{n_i}[W_i]\}$ of $n \times n$ commutative matrices isomorphic to $\bigotimes^I \{P_p^{n_i}[W_i(a_i)]\}$ are presented. Tensor product of rings of residue class polynomials is isomorphic to a ring of residue class polynomials in several variables ; for convenience we call the latter as tensor product ring. Each element in this ring is a sum of monomials arranged in lexicographic order of degrees of the variables in conjunction with an appropriately chosen mixed radix number system [56].

The description, response and implementation of $P_p^n[W(a)]$ -LSS is taken up in Chapter 3. The description of $P_p^n[W(a)]$ -LSS in terms of characterising matrices and their implementation over $P_p^n[W(a)]$ are given. $P_p^n[W(a)]$ -LSS are classified into nonsingular, singular or nilpotent systems depending upon whether their characteristic matrices are nonsingular, singular or nilpotent respectively. Conditions for the characteristic matrix A to be nonsingular, singular and nilpotent and the bound on the index of nilpotence are obtained. Expressions for the period of characteristic matrix A over various types of $P_p^n[W(a)]$ are obtained in terms of the periods of matrices over direct sum components of $P_p^n[W(a)]$. The decomposition of $P_p^n[W(a)]$ discussed in Chapter 2 has been utilised to obtain corresponding decomposition of $P_p^n[W(a)]$ -LSS.

Expressions for autonomous response and forced response of $P_p^n[W(a)]$ -LSS are derived. It is shown that the forced response of a nonsingular $P_p^n[W(a)]$ -LSS is periodic if the input is periodic. Further if J and T are the periods of the input and A respectively, the output period divides pJT .

The nature of autonomous response depends on the nature of the characteristic matrix A and is studied in detail in Chapter 4.

LSS over other families of finite commutative rings are also given. These are LSS over i) tensor product of residue class polynomial rings, ii) rings, $M_p^n[W]$ of $n \times n$ commutative matrices, iii) tensor product $\bigotimes^T \{M_p^{n_i}[W_i]\}$ of commutative rings of matrices, iv) rings $Z_p^n[W]$ of n -tuples and v) tensor product ring $\bigotimes^T \{Z_p^{n_i}[W_i]\}$ of n -tuples. It is shown that LSS over tensor product of residue class polynomial rings constitute a generalisation of $P_p^n[W(a)]$ -LSS.

Given a K th order $P_p^n[W(a)]$ -LSS implementation of $Z_p^n[W]$ -LSS, say L' , isomorphic to L is obtained. L' can alternatively be viewed as a $GF(p)$ -LSS of order nK . It is shown that the analysis of such systems of order nK , can be carried out in terms of $P_p^n[W(a)]$ -LSS of order K , thus reducing the complexity of analysis. Implementation of LSS over $\bigotimes^T \{Z_p^{n_i}[W_i]\}$ is also given. In the specific case when LSS is over $Z_p^n[W] \cong P_p^n[a^n-1]$, it is shown that multiplication of two elements from $Z_p^n[W]$ can

be carried out serially by using n -stage cyclic shift registers and atmost n modulo p adders.

LSS over isomorphic residue class polynomial rings are said to constitute a distinct class. Enumeration of distinct classes of $P_p^n[W(a)]$ -LSS, using the results of Chapter 2, on the nonisomorphic $P_p^n[W(a)]$ rings, has been given; $GF(p^n)$ -LSS constitute one of these classes.

The study of autonomous response of $P_p^n[W(a)]$ -LSS is taken up in Chapter 4. The autonomous response of $P_p^n[W(a)]$ -LSS in general, and autonomous response of nonsingular single output canonical $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$ in particular are studied. The latter response is shown to satisfy a linear recursion relation over $P_p^n[W(a)]$ and is thus a linear recursion sequence over $P_p^n[W(a)]$. Since the autonomous response is a fixed linear transformation of states, the state response of systems is studied in detail. The various aspects studied are properties of state diagram and state response, module structure of state response, bounds on number of state cycles of a nonsingular system, maximum length state sequence and isomorphism in state diagrams. The maximum possible period of a state cycle is equal to the period of A . Different LSS of the same order over a given $P_p^n[W(a)]$ are compared in terms of their Figure of merit which is defined as the ratio of maximum possible period of state cycle to the number of nonzero states.

A K th order $GF(p^n)$ -LSS whose characteristic matrix A has period $(p^{nK}-1)$ has a Figure of merit 1. For any other $P_p^n[W(a)]$ -LSS it is less than 1.

The cycle length decomposition of $P_p^n[W(a)]$ -LSS is obtained in terms of the structure of state cycles with respect to the direct sum components of the characteristic matrix A of the LSS. When the component of A is over finite field, the structure of state cycles is determined from the elementary divisors of A [4,12-14]. When the component of A is over local ring the structure of state cycle is obtained by considering an isomorphic system over $GF(p)$.

Hamming correlation properties of linear recursion sequences over $P_p^n[W(a)]$ are studied. Bounds on the values and number of levels of correlation functions are derived.

It is shown that sequences over orthogonal ideals generated by distinct orthogonal idempotents are pointwise orthogonal. Since an arbitrary sequence over a semisimple or semilocal ring can be decomposed into an internal direct sum of component sequences over orthogonal ideals, these component sequences are inherently pointwise orthogonal sequences. An arbitrary sequence over a finite field or a local ring can be decomposed into sequences over orthogonal ideals. Such orthogonal sequences can be used for modulating and multiplexing data sequences with elements from finite fields. For this purpose

the source sequences over finite fields are transformed into orthogonal sequences over orthogonal ideals in an appropriate semisimple ring. Each orthogonal sequence then modulates a maximum length sequence over the same ideal. Modulated sequences corresponding to different sources are added and transmitted as a single multiplexed sequence over the semisimple ring. The orthogonality property of sequences is used for demultiplexing the component sequences at the receiver. Demodulation is carried out by Hamming cross-correlation between each individual sequence and a corresponding reference sequence.

Chapter 5 is concerned with the application of $P_p^n[W(a)]$ -LSS for the encoding and decoding of linear polynomial and cyclic codes, which are a specific class of linear block codes over $P_p^n[W(a)]$. The development here is similar to the development in the case of codes over finite fields, the theory of which is well established [16-21,53,54]. The restrictions arising because of the presence of zero divisors are pointed out. After briefly reviewing the coding problem, linear block codes over $P_p^n[W(a)]$ are discussed. The notion of generator matrix G , parity check matrix H , are presented. Minimum Hamming distance, error correcting capability, restrictions on H of a t error correcting code, and decoding of linear block codes using decoding table are given. Polynomial code as a special case

of linear block code is taken up next. Notion of generating polynomial $g(x)$, the restrictions on the coefficients of $g(x)$, minimum distance properties, encoding and decoding principles of polynomial codes are presented. Cyclic code as a special case of polynomial code, where $g(x)$ divides (x^N-1) , is studied. Structure of cyclic codes over $P_p^n[W(a)]$, minimum distance properties, encoding and decoding principles are discussed.

The implementation of encoders for generating nonsystematic and systematic (N,K) polynomial and cyclic codes using appropriate $P_p^n[W(a)]$ -LSS are given, nonsingular, single output, canonical $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$ to generate systematic cyclic codes is explained. Variation of these encoders for generating interleaved codes are also given. In all these encoders the ring operation, that is, multiplication in Z_p^n is implemented in parallel fashion. When the ring $Z_p^n[W] \cong P_p^n[a^n-1]$, serial implementation of multiplication using cyclic shift registers is possible.

Decoders which are basically $P_p^n[W(a)]$ -LSS which perform division for computing the syndrome are used for decoding non-systematic or systematic polynomial and cyclic codes. Systematic cyclic codes are decoded using permutation decoders on the same lines as the decoding of systematic cyclic codes over finite fields [54]. Knowing the number of distinct codewords

upto cyclic shifts and their cross-correlation properties, decoding of cyclic codes can be done using Hamming cross-correlation decoders.

Summary of key results obtained and some of the aspects which could not be either pursued or taken up in this thesis are given in Chapter 6.

1.4 NOTATIONS AND CONVENTIONS

Throughout the thesis, matrices are denoted by capital letters and vectors or K-tuples by lower case letters. The product of matrix and vector or K-tuple is represented as a product of matrix and column vector or K-tuple. However, in Chapter 5 the product of matrix and K-tuple is represented by product of row K-tuple and matrix.

In the case of residue class polynomial ring $P_p^n[W(a)]$, the modulus polynomial $W(a) = a^n + w_{n-1}a^{n-1} + \dots + w_1a + w_0$, and the orthogonal idempotents in $P_p^n[W(a)]$ are written in the descending order of powers of a . An element $r(a)$ of $P_p^n[W(a)]$ is denoted by $r_0 + r_1a + \dots + r_{n-1}a^{n-1}$ in the ascending order of powers of a ; the corresponding n -tuple over $GF(p)$ is denoted by $(r_0 \ r_1 \ \dots \ r_{n-1})$. Likewise the elements of tensor product of polynomial rings are denoted using mixed radix number system, in the ascending order of powers, $\langle i_{r-1}, \dots, i_1, i_0 \rangle$ of the variables a_{r-1}, \dots, a_1, a_0 respectively.

Some notations, for example G and H , are used to represent both group and subgroup as well as generating matrix and parity check matrix respectively, as these notations are not appearing simultaneously. End of examples and proofs are indicated by $*$.

The mapping of algebraic structures or their elements are indicated by \rightarrow and the one-to-one correspondence between elements by \cong .

$P_p^n[W(a)]$, ring of residue class polynomials over $GF(p)$, is used to denote a single ring or rings depending on the context. Likewise $P_p^n[W(a)]$ -LSS may refer to a single system or systems. The elements of rings or ideals are given inside $\{ \}$.

Determinant of matrix A , is denoted by $|A|$. Transpose of matrix A is denoted by A^{tr} . Symbols 1 and 0 are used to indicate the multiplicative and additive identity, in all the polynomial rings. The corresponding identity elements in $Z_p^n[W] \cong P_p^n[W(a)]$ are an n -tuple $[1 \ 0 \ \dots \ 0]^{tr}$ and $[0 \ \dots \ 0]^{tr}$ respectively. We denote an n -tuple of zeros by $\underline{0}$ for any n . The identity elements in $M_p^n[W_1] \cong P_p^{n_1}[W_1(a)]$ are I_n , $n \times n$ identity matrix and $n \times n$ null matrix denoted by $\underline{0}$ for any n , respectively. The characterising matrices over $Z_p^n[W]$ are denoted by $\overline{A}, \overline{B}, \overline{C}$ and \overline{D} .

Whenever it is clear from the context, in the notation $M_p^n[W]$ and $Z_p^n[W] \simeq P_p^n[W(a)]$, the symbol W is omitted and written as M_p^n and Z_p^n respectively. However, in tensor product of rings W_1, W_2 are used.

$\{y\} = (y_0 \ y_1 \ \dots)$ denotes infinite sequence of period N . $y = (y_0 \ y_1 \ \dots \ y_{N-1})$ denotes finite length sequence or a codeword, over $P_p^n[W(a)]$, $y^{(i)}$ denotes components of y over local ring $P_p^{h_i n_i}[W_i^{h_i}(a)]$, z indicates an arbitrary sequence of finite length over $P_p^n[W(a)]$, $z^{(i)}$ indicates i th finite sequence, or finite sequence over i th orthogonal ideal.

CHAPTER 2

RESIDUE CLASS RINGS OF POLYNOMIALS OVER $GF(p)$: ISOMORPHISMS, DECOMPOSITION AND ENUMERATION THEOREMS

In this chapter we give necessary background material for the study of LSS over residue class rings of polynomials over the finite field $GF(p)$. The results given here pertain to isomorphisms, decomposition and enumeration theorems. The results on the isomorphism and decomposition are an adaptation of isomorphism and decomposition theorems for polynomial algebras [69,75]. As a prelude to the results given in this chapter various algebraic structures, viz., groups, rings, fields, ideals, vector spaces, modules and algebras [60-76] are briefly reviewed in Section 2.1.

Residue class rings of polynomials over $GF(p)$ are formally given in Section 2.2. First we consider residue class polynomial rings in single variables. Such rings of order p^n are denoted by $P_p^n[W(a)]$, where $W(a)$ is the modulus polynomial of degree n over $GF(p)$. Depending upon the prime factorisation of the modulus polynomial $W(a)$, the residue class polynomial rings $P_p^n[W(a)]$ are classified into fields, local rings, semi-simple and semilocal rings. The prime factorisation of $W(a)$ is also utilised to obtain an expression for the number of ideals in $P_p^n[W(a)]$. This result is used later in Chapter 4 to obtain a

bound on the number of state cycles in state diagram of $P_p^n[W(a)]$ -LSS. Since $P_p^n[W(a)]$ is also a vector space, it has a basis. The direct product of bases of two residue class polynomial rings $P_p^{n_1}[W_1(a_1)]$ and $P_p^{n_0}[W_0(a_0)]$ gives rise to a set of $n_1 n_0$ linearly independent elements which can be regarded as a basis for an $n_1 n_0$ dimensional vector space which is also a commutative ring, called the tensor product of the residue class polynomial rings $P_p^{n_1}[W_1(a_1)]$ and $P_p^{n_0}[W_0(a_0)]$ and denoted by $P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]$. Such rings are isomorphic to an appropriate residue class polynomial ring in 2 variables. Tensor product of r residue class polynomial rings can be defined likewise, which results in a ring isomorphic to a residue class polynomial ring in r variables. Tensor product of residue class polynomial rings can be regarded as a general class of residue class polynomial rings and linear sequential systems defined over tensor product of residue class polynomial rings can be regarded as a generalisation of $P_p^n[W(a)]$ -LSS.

In contrast to the case of $GF(p^n)$, all the $P_p^n[W(a)]$ of the same order are not isomorphic to each other. When two residue class polynomial rings are isomorphic to each other, structural properties, such as the number of ideals, number of units and the type of ring will be carried over to the other. Hence, it is enough if only one such ring is studied. In Section 2.3, we study the isomorphisms in residue class polynomial rings.

Specifically we study the isomorphism between (i) local rings, (ii) tensor product of primary rings and (iii) tensor product of polynomial ring and residue class polynomial ring in one variable. The isomorphisms between semisimple and semilocal rings can be proved analogously. However, to obtain this isomorphism in semisimple and semilocal rings is involved and alternatively the ring decomposition given in Section 2.4 can be utilised to obtain the isomorphism.

The decomposition of $P_p^n[W(a)]$ plays a key role in most of the analysis in this thesis. Decomposition of semisimple and semilocal rings into external direct sum and internal direct sum are given. External direct sum components are primary rings isomorphic to finite fields in the case of semisimple rings and isomorphic to either finite fields or local rings in the case of semilocal rings. Internal direct sum components of semisimple or semilocal rings are ideals generated by orthogonal idempotents; we call the collection of such ideals as orthogonal ideals. External direct sum decomposition along with isomorphisms is used in Section 2.5 in enumerating nonisomorphic residue class polynomial rings of a given order. In later chapters results on ring decomposition are utilised for obtaining condition for nilpotence of matrix A , determination of period of matrix A , computation of minimum distance of cyclic codes over semisimple ring and in the decomposition of sequences

over $P_p^n[W(a)]$ into set of sequences which have pointwise orthogonal property. Since the internal direct sum components of a given $P_p^n[W(a)]$ is isomorphic to corresponding external direct sum components, an isomorphic mapping also called ring embedding from finite field or local ring to an appropriate orthogonal ideal in semisimple or semilocal ring exists. Isomorphisms between semisimple or semilocal ring and subrings of larger semisimple or semilocal ring are also considered.

As mentioned above, residue class polynomial rings of a given order need not be isomorphic to each other. By listing all the p^n monic polynomials of degree n over $GF(p)$ in terms of their irreducible factors and using the results of Sections 2.3 and 2.4, the nonisomorphic residue class polynomial rings are enumerated in Section 2.5. It is shown that by using the notion of partition function and restricted partition functions of integers [55], it is possible to obtain the number of nonisomorphic residue class polynomial rings of order p^n without exhaustive listing of the polynomials. These results are used in Chapter 3 to obtain distinct classes of LSS defined over nonisomorphic residue class polynomial rings.

In Section 2.6, rings isomorphic to $P_p^n[W(a)]$ are taken up. In Chapter 3, LSS over these rings are defined. Such LSS are all isomorphic to LSS over $P_p^n[W(a)]$, and their analysis can be done in terms of LSS over $P_p^n[W(a)]$. Procedure for constructing rings

$M_p^n[W]$ of $n \times n$ commutative matrices over $GF(p)$, isomorphic to $P_p^n[W(a)]$ and tensor product ring $\bigotimes_{i=1}^n \{M_p^{n_i}[W_i]\}$ of $n \times n$ commutative matrices over $GF(p)$, isomorphic to $\bigotimes_{i=1}^n \{P_p^{n_i}[W_i]\}$ are given. By properly defining addition and multiplication, procedures for constructing ring $Z_p^n[W]$ of n -tuples over $GF(p)$, isomorphic to $P_p^n[W(a)]$ and tensor product rings $\bigotimes_{i=1}^n \{Z_p^{n_i}[W_i]\}$ of n -tuples over $GF(p)$ isomorphic to $\bigotimes_{i=1}^n \{P_p^{n_i}[W_i(a_i)]\}$ are also given.

2.1 REVIEW OF ALGEBRAIC STRUCTURES

To begin with we briefly review various algebraic structures, viz. groups, rings, ideals, fields, vector spaces, modules and algebras [60-73].

Groups : A set G with an operations $*$ defined for every pair of elements in G is called a group, if the following four axioms are satisfied.

- (i) Closure : for all $g_1, g_2 \in G$ $g_1 * g_2 \in G$
- (ii) Associativity : for all $g_1, g_2, g_3 \in G$; $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$
- (iii) Identity : G contains an element e called the identity of G such that for every $g \in G$, $e * g = g * e = g$
- (iv) Inverse : For every $g \in G$ there is an element $g^{-1} \in G$ called inverse of g such that $g * g^{-1} = e$.

G is an abelian group (commutative group) if the following axiom is also satisfied.

- (v) Commutativity for all $g_1, g_2 \in G$ $g_1 * g_2 = g_2 * g_1$.

When the operation is addition denoted by $+$, G is an additive group; e is the zero of G denoted by 0 and inverse of g is $-g$.

When the operation is multiplication denoted by $.$ or with no symbol, G is a multiplicative group. Identity of G is 1 and inverse of $g \in G$ is g^{-1} .

The number of elements in G is called the order of G and is denoted by $|G|$. If $|G|$ is finite, G is called a finite group.

A nonempty subset H of a group G is a subgroup of G if H itself forms a group.

Let G be a group, G is cyclic if there exists an element g of G such that every element g_i of G can be written in the form g^n for some integer n . g is then called a generator of G .

Let g be an element of group G . The subset of all elements g^n is a subgroup of G which is cyclic.

Let $H = \{h_0, h_1, \dots, h_{r-1}\}$ be any subgroup of order r of a commutative group G . A table of G modulo H is constructed by listing H as a first row placing $h_0 = 0$ in the left most portion. Thus

$$h_0, h_1, \dots, h_{r-1}$$

form the first row of the table. Then some element $g_1 \in G$ which is not in the first row is selected and a new row or a coset is formed by adding g_1 to each h_i ; $i = 0, 1, \dots, r-1$ as follows :

$$\begin{array}{cccc}
 h_0 & h_1 & \dots & h_{r-1} \\
 h_0+g_1 & h_1+g_1 & \dots & h_{r-1}+g_1
 \end{array}$$

h_0+g_1 is called the coset leader. A new element $g_2 \in G$ not in the above two rows is then selected and the third coset is formed. The process is continued until each element of G is somewhere in the table. With this no word in the table is duplicated. It can be shown that elements g_i and $g_j \in G$ are in the same coset iff $g_i - g_j \in H$. The cosets are also called as residue classes of G with respect to H , which has a group structure.

Rings : A set R with two binary operations is called a ring if for every pair of elements the following four axioms are satisfied.

- (i) R is additive abelian group
- (ii) Closure : for all $r_1, r_2 \in R$, $r_1 r_2 \in R$
- (iii) Associativity : for all $r_1, r_2, r_3 \in R$,

$$r_1(r_2 r_3) = (r_1 r_2)r_3$$
- (iv) Distributivity : for all $r_1, r_2, r_3 \in R$,

$$r_1(r_2 + r_3) = r_1 r_2 + r_1 r_3$$

and $(r_2 + r_3)r_1 = r_2 r_1 + r_3 r_1$

R is a commutative ring if the following axiom is also satisfied.

(v) Commutativity : for all $r_1, r_2 \in R$, $r_1 r_2 = r_2 r_1$.

A ring R is called a finite ring if the order of R is finite; otherwise, it is called an infinite ring. If R contains multiplicative identity 1 such that $\forall r \in R$, $1 \cdot r = r \cdot 1 = r$, then R is called a ring with identity.

If an element $r \in R$ has a multiplicative inverse we call r a unit in R .

If r and s are nonzero elements of R and $rs = 0$, r and s are called proper divisors of zero. A unit in R cannot be a zero divisor.

A commutative ring in which there are no zero divisors is called an integral domain or simply a domain.

The set of integers, with the usual addition and multiplication operations, constitutes an infinite commutative ring with identity. This ring is called the ring of integers and is denoted by \mathbb{Z} . The set of all even integers with the usual addition and multiplication constitutes an infinite commutative ring without identity. Both of these rings are also integral domains.

An integral domain in which every nonzero element has a multiplicative inverse constitutes a field,

thus, A set F with two binary operations is called a Field if F is a commutative ring with identity 1 such that for every $\alpha \in F$

$$1\alpha = \alpha 1$$

and every nonzero $\alpha \in F$ has an inverse α^{-1} such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$.

The nonzero elements in F constitute a cyclic group under multiplication. A finite integral domain is a field.

Example 2.1.1 : (i) The set of all complex numbers with the usual rules of addition and multiplication of complex numbers constitute an infinite field.

(ii) Set of all integers $\{0, 1, \dots, p-1\}$, p a prime with addition and multiplication operations defined such that the result is the remainder after division by p , constitutes a finite field of order p denoted by $GF(p)$. (the operations are called modulo p operations). *

Ideals in the ring R : A subset J of a ring R is called left (right) ideal iff (i) J is an additive subgroup of R ; that is, $j_1, j_2 \in J$ implies $j_1 - j_2 \in J$ and (ii) $r \in R$, $j \in J$ implies $rj \in J$ ($jr \in J$). Ideals which are both right and left are called two sided ideals. Since we are interested in commutative rings these distinctions, namely, left, right and two sided are immaterial and all ideals are written as left ideals.

Intersection of ideals (as sets) is again an ideal. If r_1, r_2, \dots, r_n are elements of a ring R , then we denote by $\langle r_1, r_2, \dots, r_n \rangle$ the intersection of all ideals in R containing these elements. r_1, r_2, \dots, r_n are called the generators of the ideal. An ideal J generated by a single element r of R

is called a principal ideal and is denoted by $\langle r \rangle$. We note that the ideal $\langle 1 \rangle$ generated by the multiplicative identity 1 is the ring R itself.

An ideal J in R which is neither $\langle 0 \rangle$ nor $\langle 1 \rangle$ is called a proper ideal in R . An ideal J is called a simple ideal if it is not $\langle 0 \rangle$ and does not contain a proper ideal.

If every ideal in R is principal, then R is called a principal ideal ring. A principal ideal ring which is also an integral domain is called a principal ideal domain. Ring of integers is an example of principal ideal domain.

Residue class rings :

Let R be a commutative ring and J one of its ideals. J is also a subgroup of R and cosets can be formed. The family of sets $r+J$, $r \in R$ are the residue classes of R with respect to J . Two residue classes $r+J$ and $r'+J$ are same iff $r-r' \in J$. The residue classes form a ring called residue class ring, or quotient ring and is denoted by R/J . The addition and multiplication in R/J are defined as follows :

$$(r+J) + (s+J) = (r+s+J)$$

$$(r+J) \cdot (s+J) = (rs+J)$$

In the quotient ring R/J , $r_1 = r_2$ modulo J implies $(r_1 - r_2) \in J$. If J is a principal ideal $J = \langle r \rangle$, then $r_1 = r_2$ modulo J is simply written as $r_1 = r_2$ modulo r .

Example 2.1.2 :

Consider the ring Z of integers. 6 is an element of Z and $\langle 6 \rangle$ is the principal ideal generated by 6 , i.e. $\langle 6 \rangle = \{ \dots -6, -12, 0, 6, 12, \dots \}$. The residue classes of Z with respect to $\langle 6 \rangle$ are

$$0+\langle 6 \rangle, 1+\langle 6 \rangle, 2+\langle 6 \rangle, 3+\langle 6 \rangle, 4+\langle 6 \rangle, 5+\langle 6 \rangle .$$

Denoting $\bar{i} = i+\langle 6 \rangle$ the residue class ring Z_6 of integers modulo 6 is $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. For convenience we write the residue classes without bar over the elements. Thus, $Z_6 = \{0, 1, 2, 3, 4, 5\}$. *

An element $e \neq 1$, in R such that $e^2 = e$ is called an idempotent element in R . If two idempotents e_i and e_j are such that $e_i \cdot e_j = 0$, then, they are said to be orthogonal. If e is an idempotent, then, $(1-e)$ is also an idempotent because, $(1-e)^2 = (1-2e+e^2) = (1-e)$. Furthermore, since $(1-e) \cdot e = 0$, $(1-e)$ and e are orthogonal. The orthogonal idempotents of R generate proper ideals. Consider ideals J_i and J_j generated by distinct orthogonal idempotents e_i and e_j respectively. The elements of J_i and J_j are multiples of e_i and e_j , respectively. Hence, if r_i and r_j are elements from ideals J_i and J_j respectively, $(J_i \neq J_j)$, then by the property of orthogonal idempotents $r_i \cdot r_j = 0$. Thus elements from different ideals generated by orthogonal idempotents annihilate each other. For the sake of convenience the ideals generated by orthogonal idempotents are

called orthogonal ideals.

In what follows we consider finite commutative rings with identity unless otherwise specified.

Example 2.1.3 :

Consider the residue class ring Z_6 of integers, modulo 6, $Z_6 = \{0,1,2,3,4,5\}$. In this ring, 3 and 4 are the orthogonal idempotents because $3^2 = 3$ modulo 6 and $4^2 = 4$ modulo 6, and $3 \cdot 4 = 12 = 0$ modulo 6. The ideals $J_1 = \langle 3 \rangle = \{0,3\}$; and $J_2 = \langle 4 \rangle = \{0,4,2\}$, generated by the orthogonal idempotents 3 and 4 constitute orthogonal ideals in Z_6 . The elements from J_1 and J_2 annihilate each other. *

An ideal J_p in R is called a prime ideal if $J_p \neq \langle 1 \rangle$ and $r_1 r_2 \in J_p$ implies $r_1 \in J_p$ or $r_2 \in J_p$. A ring with at most one prime ideal is called a primary ring. In the ring Z of integers, the ideals $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 5 \rangle$, ... generated by prime integers 2, 3, 5 ... are prime ideals. Since Z has more than one prime ideal, it is not a primary ring. On the otherhand consider the residue class ring of integers modulo 5 i.e., $Z_5 = \{0,1,2,3,4\}$. Z_5 does not have any proper ideal in it. Hence, by definition it is a primary ring. Since all the nonzero elements in Z_5 have multiplicative inverse and multiplication is commutative, Z_5 is a finite field of order 5.

An ideal J_m in R is maximal if $J_m \neq \langle 1 \rangle$ and there is no ideal J such that $J_m \subset J \subset \langle 1 \rangle$. A maximal ideal is prime but not conversely in general. In the ring $Z_8 = \{0,1,2,3,4,5,6,7\}$ the ideals are $\langle 2 \rangle = \{0,2,4,6\}$; $\langle 4 \rangle = \{0,4\}$. Note that, $\langle 2 \rangle \neq \langle 1 \rangle$. Further, $\langle 2 \rangle$ consists of all the zero divisors in Z_8 and $\langle 2 \rangle$ is not contained in any other proper ideal in Z_8 . Hence, $\langle 2 \rangle$ is a unique maximal ideal.

A ring with a unique maximal ideal is called a local ring; this unique maximal ideal consists of all non-unit elements of the ring. The ring Z_8 is therefore a local ring.

A ring with finite number of maximal ideals is called a semilocal ring. In the residue class ring Z_{12} of integers modulo 12, the ideals are $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$ and $\langle 6 \rangle$. It can be seen that $\langle 2 \rangle = \{0,2,4,6,8,10\}$ and $\langle 3 \rangle = \{0,3,6,9\}$ are the two maximal ideals. Hence, Z_{12} is a semilocal ring.

Let J be an ideal in R . The set of all elements r of R such that some positive power of r is in J is called the radical of J , denoted by $\text{rad } J$. If R is considered as an ideal, then its radical is the ring itself.

An element $r \in R$, such that $r^n = 0$ for some positive integer n , is called a nilpotent element. The set J_N of all nilpotent elements in a ring R is an ideal; this ideal is called the nil-radical of R . J_N is the intersection of all the prime ideals of R . In the residue class ring Z_{12} of integers modulo 12, the

prime ideals are $\langle 2 \rangle$ and $\langle 3 \rangle$. The intersection of these prime ideals, viz., $\{0, 6\}$ is the nilradical of Z_{12} .

A semilocal ring whose nilradical J_N is $\langle 0 \rangle$ is called a semisimple ring. In Z_6 , the prime ideals are $\langle 2 \rangle = \{0, 2, 4\}$ and $\langle 3 \rangle = \{0, 3\}$. The nilradical J_N of Z_6 is the intersection of these prime ideals, i.e., $J_N = \langle 0 \rangle$. Z_6 is therefore a semisimple ring.

A ring R is called a simple ring iff, it has no proper ideals. The only ideals in simple ring R are $\langle 0 \rangle$ and $\langle 1 \rangle$.

The foregoing terms on rings and ideals are further illustrated below in terms of the general residue class ring Z_m of integers modulo an arbitrary integer m .

Residue class ring Z_m of integers modulo m with addition and multiplication modulo m constitutes a finite commutative ring with identity. The order of this ring is m .

$$Z_m = \{0, 1, 2, \dots, m-1\}$$

An element $r \in Z_m$, represents a class of integers of the form $j^m + r$ where j is any positive integer.

(i) For $m = p$; a prime integer, Z_p does not have a proper ideal. Hence, by definition Z_p is a primary ring as well as a simple ring. Further, since all the non-zero elements of Z_p have multiplicative inverse, it is a finite field of order p .

(ii) For $m = p^n$; power of a prime integer, $Z_{p^n} = \{0, 1, \dots, p^n - 1\}$ is a finite commutative ring of order $m = p^n$ with identity. Any multiple of p is a zero divisor and is a nilpotent element. All the factors of p^n generate ideals which are contained in $\langle p \rangle$. Hence, $\langle p \rangle$ is the unique maximal ideal which contains all the zero divisors in Z_m , and consequently, Z_{p^n} is a local ring. $\langle p \rangle$ is also a unique prime ideal in Z_{p^n} . Hence by definition Z_{p^n} is also a primary ring.

(iii) For $m = p_1^{h_1} p_2^{h_2} \dots p_\nu^{h_\nu}$, product of powers of distinct prime integers, $Z_{p_1^{h_1} p_2^{h_2} \dots p_\nu^{h_\nu}} = Z_m = \{0, 1, \dots, m-1\}$ is a finite commutative ring with identity. Each prime integer p_i , $i = 1, 2, \dots, \nu$ generates a maximal ideal. Hence by definition Z_m is a semilocal ring. Elements of Z_m which contain $\prod_{i=1}^{\nu} p_i$ as factors are nilpotent elements in Z_m .

(iv) For $m = p_1 p_2 \dots p_\nu$: product of distinct prime integers, $Z_{p_1 p_2 \dots p_\nu} = Z_m = \{0, 1, \dots, (m-1)\}$ is a finite commutative ring with identity. Each prime integer p_i generates a maximal ideal (which is also prime ideal). Hence, by definition Z_m is a semilocal ring. Since m is a product of prime integers this ring has additional property. Consider an element $r \in Z_m$. Any power of r is not a multiple of m and hence not zero modulo m . Thus, there is no nonzero nilpotent element in Z_m . Hence, Z_m is semisimple.

Ring Homomorphisms

Let R and S be two rings and let

$\phi : R \rightarrow S$ be a mapping which

satisfies $\phi(a+b) = \phi(a) \oplus \phi(b)$

$$\phi(a \cdot b) = \phi(a) * \phi(b) .$$

where $a, b \in R$ and $+, \cdot$, operations in R and $\oplus, *$ operations in S . Then ϕ is a ring homomorphism. If ϕ is injective (one to one) it is called ring monomorphism, sometimes also called as embedding of R into S . If ϕ is surjective (onto) it is called ring epimorphism. If ϕ is bijective (one to one and onto) it is called a ring isomorphism and R and S are called isomorphic rings.

The set $\{r \in R \mid \phi(r) = 0\}$ is called Kernel of ϕ and is denoted by $\text{Ker}\phi$. $\text{Ker}\phi$ is an ideal in R . The residue class ring. $R/\text{Ker}\phi$ is isomorphic to image of ϕ , that is, $\phi(R)$. If $\text{Ker}\phi = 0$, then ϕ is one to one. If $R = S$, a homomorphism (isomorphism)

$$\phi : R \rightarrow R$$

is called an endomorphism (automorphism).

Direct Sums of Rings

Let R_1, R_2, \dots, R_n be a finite collection of rings and R

the Cartesian product (set of all ordered ν -tuples with one element each from R_i 's) of R_i 's. Then with component-wise addition and multiplication of elements from R , that is,

$$(r_1, \dots, r_\nu) + (s_1, \dots, s_\nu) = (r_1+s_1, \dots, r_i+s_i, \dots, r_\nu+s_\nu)$$

$$(r_1 \dots r_\nu) \cdot (s_1 \dots s_\nu) = (r_1 s_1 \dots r_\nu s_\nu)$$

where the operations on the right hand side are understood to be operations in the respective rings, R becomes a ring with $(0, 0, \dots, 0)$ as the additive identity and $(-r_1, -r_2, \dots, -r_\nu)$ as the additive inverse of (r_1, r_2, \dots, r_ν) .

The coordinate projections,

$\phi_i : (r_1, \dots, r_i \dots r_\nu) \longrightarrow r_i$ are ring epimorphisms from R into R_i

The above ring R is called the external direct sum of the rings R_1, R_2, \dots, R_ν and is denoted by

$$R = R_1 \oplus R_2 \oplus \dots \oplus R_\nu$$

For each $i = 1, 2, \dots, \nu$ let J_i be the set of all elements $(0 \dots r_i 0 \dots 0)$ of R that is the set of all ν -tuples having zero entries except possibly in the i th place. Each J_i is an ideal in R . Furthermore, in J_i , the element $e_i = (0 \dots 1 \dots 0)$; 1 in i th position, is an idempotent since $(0 \dots 1 \dots 0)(0 \dots 1 \dots 0) = (0 \dots 1 \dots 0)$

and $e_i \cdot e_j = 0$ $i \neq j$. Hence e_i , $i = 1, 2, \dots, n$ are orthogonal idempotents, and J_i ; $i = 1, 2, \dots, n$ are such that elements from different ideals J_i and J_j $i \neq j$, mutually annihilate. Thus J_1, J_2, \dots, J_n are a set of orthogonal ideals. The coordinate projection ϕ_i restricted to J_i induces an isomorphism between J_i and R_i .

The ideals J_1, J_2, \dots, J_n have the following properties

- i) Since $\sum_{j \neq i} J_j$ consists of all elements of R whose i th component is zero; $J_i \cap \sum_{j \neq i} J_j = \langle 0 \rangle$ and (ii) $R = J_1 + J_2 + \dots + J_n$

Then R is said to be the internal direct sum of the ideals J_i and is written as $R = J_1 + J_2 + \dots + J_n$.

The external direct sum may be thought of as a way of building up more complicated rings from given ones and the internal direct sum as a way of breaking a given ring into simpler components. When R is the internal direct sum of its ideals J_1, J_2, \dots, J_n having the above mentioned two properties every element $r \in R$ has a unique representation in the form

$$r = r_1 + r_2 + \dots + r_n \quad \text{with } r_i \in J_i.$$

Example 2.1.4

Consider simple rings $Z_2 = \{0,1\}$, $Z_3 = \{0,1,2\}$

The external direct sum $Z' = Z_2 \oplus Z_3 = \{(00), (10), (01), (11), (02), (12)\}$ with pointwise addition and multiplication modulo 2 and 3 respectively constitute a ring. The ideals in Z' are

$$J'_1 = \{(00), (10)\}$$

$$J'_2 = \{(00), (01), (02)\} .$$

We note that, $J'_1 \cap J'_2 = 0$ and $Z' = J'_1 + J'_2$ (internal direct sum of ideals J'_1 and J'_2) also $J'_1 \simeq Z_2$ and $J'_2 \simeq Z_3$.

*

Example 2.1.5

Consider semisimple ring $Z_6 = \{0,1,2,3,4,5\}$

We show that $Z_6 \simeq Z_2 \oplus Z_3 = Z'$. The one-to-one correspondence between the elements of Z_6 and Z' are obtained by the following mapping

$$r \in Z_6 \mapsto (r_1 = r \text{ modulo } 2, r_2 = r \text{ modulo } 3) \in Z' .$$

The orthogonal idempotents in Z_6 are 3 and 4. Given $(r_1, r_2) \in Z'$ the corresponding element r in Z_6 is obtained using the Chinese remainder theorem (Appendix E)

$$r = 3r_1 + 4r_2 \text{ modulo } 6 .$$

The one-to-one correspondence between the elements of Z_6 and Z' is given below.

$$0 \cong (0,0) ; \quad 1 \cong (1,1), \quad 2 \cong (0,2) ; \quad 3 \cong (1,0);$$

$$4 \cong (0,1); \quad 5 \cong (1,2)$$

Z_6 has two simple ideals $J_1 = \{0,3\} \cong Z_2$ and $J_2 = \{0,2,4\} \cong Z_3$

Furthermore $J_1 \cap J_2 = \langle 0 \rangle$ and $Z_6 = J_1 + J_2$. Z_6 is the internal direct sum of simple ideals. Also Z_6 is isomorphic to the external direct sum of simple rings Z_2 and Z_3 that is

$Z_6 \cong Z_2 \oplus Z_3$. These are general properties of semisimple rings, in addition to their nilradical being zero. *

In general when m is a product of relatively prime integers m_1, m_2, \dots, m_ν we have $Z_m \cong Z_{m_1} \oplus Z_{m_2} \oplus \dots \oplus Z_{m_\nu}$. When m_1, m_2, \dots, m_ν are distinct prime integers Z_i are simple; $i = 1, 2, \dots, \nu$ and the external direct sum is then isomorphic to semisimple Z_m .

Vector Spaces

Let V be an abelian group and F a field. Then V is called a vector space over F if the following postulates are satisfied.

1. Closure : for all $\beta \in F$ and $v \in V$, βv is defined and is in V
2. Associativity for all β, γ in F and v in V $(\beta \gamma)v = \beta(\gamma v)$

3. Distributivity : for all β, γ in F and u, v in V

$$\beta(u+v) = \beta u + \beta v \quad \text{and}$$

$$(\beta+\gamma)v = \beta v + \gamma v$$

4. Identity : for all v in V $1v = v$.

Elements of V are called vectors and elements of F are called scalars.

Modules

Module is a generalisation of the notion of a vector space; the field F is replaced by a ring R and is denoted by R -module. A ring R is an R module over itself, with the scalar product defined as the ring product. We are interested only in commutative rings in which case there is no distinction between left and right R modules.

A map $\phi : S \rightarrow S'$ between R modules S and S' is an R -module homomorphism iff

$$\phi(s+s') = \phi(s) + \phi(s') \quad s, s' \in S$$

$$\phi(\beta s) = \beta \phi(s) \quad s \in S; \beta \in R$$

An R -module S is said to be finitely generated iff every element of s can be represented as $s = \sum_{i=1}^k r_i(s) s_i$

$$s_i \in S \quad r_i(s) \in R ;$$

the $r_i(s)$ are not necessarily unique. If they are unique for all s , then we call S a free module and the set $\{s_1, s_2, \dots, s_k\}$ is a basis for S . k is called the rank of the module.

In a free module, $\sum_{i=1}^m r_i(s) s_i = 0$ implies $r_i(s) = 0$. A submodule S_1 of an R -module S is a subgroup of S such that $r \in R$ and $s_1 \in S_1$ implies $rs_1 \in S_1$.

Example 2.1.6

The set of all K -tuples over R is an R -module of rank K , with a basis s_1, s_2, \dots, s_K where $s_i = (00 \dots 01 0 \dots 00)$ with 1 in the i th position. *

Algebras : A linear algebra over a field F is a set S which is both a ring and a vector space over F in such a manner that the additive group structure are the same and the axiom $\beta(s_1 s_2) = (\beta s_1) s_2 = s_1 (\beta s_2)$ is satisfied for all $s_1, s_2 \in S$ and $\beta \in F$.

2.2 RINGS OF POLYNOMIALS OVER $GF(p)$

Consider expressions of the form $f(x) = f_0 + f_1 x + \dots + f_n x^n$ where $f_i \in GF(p)$, such that all but finite number of f_i are zeros. Let S denote the set of all such expressions. The elements of S are called polynomials in indeterminate or variable x . If $f(x)$ is a nonzero polynomial and if n is the greatest integer such that $f_n \neq 0$; $n \geq 0$ then n is called the degree of $f(x)$

and f_0, f_1, \dots, f_n are called the coefficients of $f(x)$. f_n is called the leading coefficient of $f(x)$. If $f_n = 1$ the polynomial $f(x)$ is called monic. We note that,

i) S is an additive abelian group; $f(x), g(x) \in S$,

$$f(x) + g(x) = \sum_{i=0}^{n'} (f_i + g_i) x^i ; \text{ where } n' \text{ is the maximum of}$$

the degree of $f(x)$ and $g(x)$, and the addition of coefficients f_i and g_i is modulo p , 0 polynomial constitutes the additive identity.

ii) S is closed under multiplication; $f(x), g(x) \in S$,

$$f(x) \cdot g(x) = h(x) = \sum_k h_k x^k \in S; \text{ where}$$

$$h_k = \sum_{i+j=k} f_i g_j ; k = 0, 1, \dots$$

iii) Multiplication is associative :

$$\begin{aligned} \text{for all } f(x), g(x), h(x) \in S, \quad f(x)(g(x)h(x)) \\ = (f(x)g(x)) h(x) \end{aligned}$$

iv) Multiplication is distributive over addition

$$\begin{aligned} \text{for all } f(x), g(x), h(x) \in S, \quad f(x)(g(x)+h(x)) \\ = f(x) g(x) + f(x) h(x) \end{aligned}$$

$$\text{and } (g(x)+h(x))f(x) = g(x)f(x)+h(x)f(x) .$$

Further $f(x)g(x) = g(x)f(x)$ and 1 is the multiplicative identity such that $1 \cdot f(x) = f(x) \cdot 1 = f(x)$.

Thus S satisfies the axioms of a commutative ring with identity. The ring S is denoted by $GF(p)[x]$ and is referred to as polynomial ring in variable x over $GF(p)$. $GF(p)[x]$ is a principal ideal ring.

Likewise the set of all polynomials $f(x_{r-1}, x_{r-2}, \dots, x_1, x_0)$ over $GF(p)$ in r variables $x_{r-1}, x_{r-2}, \dots, x_1, x_0$ constitutes a commutative ring with identity, denoted by $GF(p)$

$GF(p)[x_{r-1}, x_{r-2}, \dots, x_1, x_0]$. However, for $r \geq 2$, this is not a principal ideal ring.

2.2.1 Residue Class Ring of Polynomials over $GF(p)$ in One Variable

Let $W(x) \in GF(p)[x]$ be of degree n . Then the set of all multiples of $W(x)$ constitutes a principal ideal in $GF(p)[x]$. We denote this ideal by $\langle W(x) \rangle$. The residue classes of polynomials modulo $W(x)$, denoted by $\frac{GF(p)[x]}{\langle W(x) \rangle}$, is a finite commutative ring of order p^n , and with identity. For convenience we denote this ring by $P_p^n[W(a)]$, where a^i represents the residue class containing x^i , i.e., $x^i + \langle W(x) \rangle$; $W(a)$ is called the modulus polynomial.

The ring $P_p^n[W(a)]$ is not necessarily a domain. It may have divisors of zero which are polynomials that have a factor in common with the polynomial $W(a)$. The units in $P_p^n[W(a)]$ are

polynomials that are relatively prime to $W(a)$. Every nonzero element of the ring $P_p^n[W(a)]$ is either a unit or a zero divisor.

If $W(a)$ is irreducible over $GF(p)$, then $P_p^n[W(a)]$ is a finite field called Galois field of order p^n , which is denoted by $GF(p^n)$.

The set of all polynomials in $P_p^n[W(a)]$ constitutes a vector space over $GF(p)$. The set $\{1, a, \dots, a^{n-1}\}$ is a basis of this vector space. Hence $P_p^n[W(a)]$ is also a commutative algebra over $GF(p)$. It is called the polynomial algebra generated by $W(a)$ [75].

Example 2.2.1

Consider $P_2^3[a^3+a^2+a+1]$ with $\{1, a, a^2\}$ as a basis. The set of all polynomials of degree less than 3 with arithmetic modulo 2 and modulo (a^3+a^2+a+1) denoted by modulo, $[2, a^3+a^2+a+1]$ constitutes $P_2^3[a^3+a^2+a+1]$. *

Depending on the prime factorisation of $W(a)$, $P_p^n[W(a)]$ may be classified into four categories :

(i) if $W(a)$ is an irreducible polynomial over $GF(p)$, then $P_p^n[W(a)]$ does not have proper ideals. Hence $P_p^n[W(a)]$, by definition is a simple ring or primary ring. In particular $P_p^n[W(a)]$ is $GF(p^n)$.

(ii) if $W(a)$ is a power of an irreducible polynomial $W_1^h(a)$, where $W_1(a)$ is irreducible, then ideal generated by $W_1(a)$ is

the maximal ideal in $P_p^n[W(a)]$. Hence, $P_p^n[W(a)]$ is a local ring. $P_p^n[W(a)]$ has only one prime ideal $\langle W_1(a) \rangle$, hence is also a primary ring.

(iii) if $W(a)$ is a product of irreducible polynomials, i.e., $W(a) = \prod_{i=1}^v W_i(a)$; $W_i(a)$ irreducible over $GF(p)$. Then, $P_p^n[W(a)]$ has finite number of maximal ideals namely $\langle W_1(a) \rangle, \langle W_2(a) \rangle, \dots, \langle W_v(a) \rangle$. Hence, it is a semilocal ring. In this ring any nonzero element $r(a)$ is not a multiple of $W(a)$ and hence any power of $r(a)$ modulo $W(a)$ is not zero. Therefore, zero is the only nilpotent element in this ring. The nilradical of $P_p^n[W(a)]$ is thus $\langle 0 \rangle$. Hence, $P_p^n[W(a)]$ is a semisimple ring.

(iv) If $W(a)$ is a product of powers of irreducible polynomials $W(a) = \prod_{i=1}^v W_i^{h_i}(a)$; $W_i(a)$ irreducible over $GF(p)$. $P_p^n[W(a)]$ has finite number of maximal ideals generated by $W_i(a)$, $i = 1, 2, \dots, v$. Hence is a semilocal ring. Elements in this ring which are multiples of $\prod_{i=1}^v W_i(a)$ are nilpotent elements.

The above classification of $P_p^n[W(a)]$ based on prime factorisation of $W(a)$ is summarised in Table 2.2.1.

Example 2.2.2

i) $P_2^2[a^2+a+1] \cong GF(2^2)$.

Table 2.2.1 Classification of $P_p^n[W(a)]$

Type of $W(a)$	Type of $P_p^n[W(a)]$	Remarks
Irreducible polynomial	$P_p^n[W(a)]$ is a field of order p^n	$P_p^n[W(a)]$ is both a simple ring and a primary ring
Power of an irreducible polynomial	$P_p^n[W(a)]$ is a local ring	$P_p^n[W(a)]$ is a primary ring
Product of irreducible polynomials	$P_p^n[W(a)]$ is a semisimple ring	Nil radical N of $P_p^n[W(a)]$ is $\langle 0 \rangle$
Product of powers of irreducible polynomials	$P_p^n[W(a)]$ is a semilocal rings	$P_p^n[W(a)]$ has nonzero nil-radical

- (ii) $P_2^3[a^3+1]$ is a semisimple ring. The only nilpotent element is zero. This is also a semilocal ring; $\langle a+1 \rangle$ and $\langle a^2+a+1 \rangle$ are the maximal ideals.
- (iii) $P_2^6[a^6+1]$ is a semilocal ring; $\langle a+1 \rangle$, $\langle a^2+a+1 \rangle$ are the maximal ideals.
- (iv) $P_2^4[a^4+a^2+1]$ is a local ring, $\langle a^2+a+1 \rangle$ is the only maximal ideal.
- (v) $P_p^n[a^{p^n}+1]$, n any integer, is a local ring $\langle a+1 \rangle$ is the only maximal ideal.

Given a ring $P_p^n[W(a)]$, where $W(a) = \prod_{i=1}^n W_i^{h_i}(a)$, $W_i(a)$ irreducible over $GF(p)$, we find the number of proper ideals in $P_p^n[W(a)]$. This result is used in determining the minimum number of state cycles in the enumeration of state cycles discussed in Section 4.2. *

Theorem 2.2.1

The number of proper ideals h in $P_p^n[W(a)]$ as defined above is given by

$$h = \left[\prod_{i=1}^n (h_i+1) \right] - 2$$

Proof

In the ring $P_p^n[W(a)]$, the generators of the ideals are all the proper divisor of $W(a)$. Hence, the number of proper ideals in $P_p^n[W(a)]$ is equal to the number of proper divisors of $W(a)$; that is divisors of $W(a)$ excluding 1 and $W(a)$.

We have $W(a) = w_1^{h_1}(a) w_2^{h_2}(a) \dots w_\nu^{h_\nu}(a)$

A typical divisor $g(a)$ of $W(a)$ may have the following form

$$g(a) = \prod_{i=1}^{\nu} w_i^{j_i}(a) \text{ where}$$

$$0 \leq j_1 \leq h_1 \quad \text{i.e.} \quad j_1 \text{ can take } (h_1+1) \text{ values}$$

$$0 \leq j_2 \leq h_2 \quad \text{i.e.} \quad j_2 \text{ can take } (h_2+1) \text{ values}$$

.....

$$0 \leq j_\nu \leq h_\nu \quad \text{i.e.} \quad j_\nu \text{ can take } (h_\nu+1) \text{ values.}$$

$$\text{The number of such divisors} = \prod_{i=1}^{\nu} (h_i+1)$$

For $j_i = 0 \quad i = 1, 2, \dots, \nu$ the divisor $g(a) = 1$

For $j_i = h_i \quad i = 1, 2, \dots, \nu$ the divisor $g(a) = W(a)$.

Hence, the number of proper divisors of $W(a)$ is $h = \left[\prod_{i=1}^{\nu} (h_i+1) - 2 \right]$ which is equal to the number of ideals in $P_p^n[W(a)]$.

*

Example 2.2.3

Consider $P_2^6[a^6+1]$, $(a^6+1) = (a+1)^2 (a^2+a+1)^2$

Here $h_1 = 2, h_2 = 2$. Hence, number of ideals in $P_2^6[a^6+1]$ is

$(2+1)^2 - 2 = 7$. They are $\langle a+1 \rangle, \langle a^2+a+1 \rangle, \langle (a+1)^2 \rangle, \langle (a^2+a+1)^2 \rangle, \langle (a+1)(a^2+a+1) \rangle, \langle (a+1)^2 (a^2+a+1) \rangle, \langle (a+1)(a^2+a+1)^2 \rangle$.

*

Corollary 2.2.1

Number of ideals in a local ring $P_p^n[W(a)]$, where $W(a) = w_1^{h_1}(a)$, and $w_1(a)$ is an irreducible polynomial, is given by (h_1-1) .

Proof

From the Theorem 2.2.1, number of ideals in this case $= (h_1+1)-2 = (h_1-1)$. The ideals are

$$\langle W_1(a) \rangle, \langle W_1^2(a) \rangle, \dots, \langle W_1^{h_1-1}(a) \rangle.$$

*

Corollary 2.2.2

Number of ideals in a semisimple ring $P_p^n[W(a)]$, where $W(a) = \prod_{i=1}^v W_i(a)$ and $W_i(a)$ is irreducible over $GF(p)$, $i = 1, 2, \dots, v$ is given by $(2^v - 2)$.

Proof

Using the result of the Theorem, ^{2.2.1} we have for $h_i = 1, \forall i$, the number of ideals in $P_p^n[W(a)]$ is equal to

$$\left[\prod_{i=1}^v (h_i+1) \right] - 2 = (2^v - 2).$$

*

Example 2.2.4

Consider the ring $P_2^3[a^3+1]$. $(a^3+1) = (a+1)(a^2+a+1)$, $h_1 = 1, h_2 = 1$, Number of ideals in this ring is $(2^2-2) = 2$. They are $\langle a+1 \rangle$ and $\langle a^2+a+1 \rangle$.

*

2.2.2 Tensor Product of Rings of Residue Class Polynomials Over $GF(p)$ in One Variable

Consider the finite field $GF(p)$. Over this field let

$$W_1(a_1) = a_1^{n_1} + w_{1,n_1-1}a_1^{n_1-1} + \dots + w_{1,1}a_1 + w_{1,0} \quad \text{and}$$

$W_0(a_0) = a_0^{n_0} + w_{0,n_0-1}a_0^{n_0-1} + \dots + w_{0,1}a_0 + w_{0,0}$ be two polynomials in variable a_1 and a_0 respectively. The residue class polynomial rings $P_p^{n_1}[W_1(a_1)]$ and $P_p^{n_0}[W_0(a_0)]$ considered as algebras, generated by $W_1(a_1)$ and $W_0(a_0)$ respectively, have the following set of monomials as their basis

$$\{1_{a_1}, a_1, a_1^2, \dots, a_1^{n_1-1}\}; a_1^{i_1} \in P_p^{n_1}[W_1(a_1)]; i_1=1, 2, \dots, n_1-1 \quad (2.2.1)$$

and

$$\{1_{a_0}, a_0, a_0^2, \dots, a_0^{n_0-1}\}; a_0^{i_0} \in P_p^{n_0}[W_0(a_0)]; i_0=1, 2, \dots, n_0-1 \quad (2.2.2)$$

where 1_{a_1} and 1_{a_0} are the identity elements in $P_p^{n_1}[W_1(a_1)]$ and $P_p^{n_0}[W_0(a_0)]$ respectively.

Consider the following lexicographically ordered set of direct product of basis elements given by (2.2.1) and (2.2.2)

$$\begin{aligned} &\{1_{a_1} \otimes 1_{a_0}, 1_{a_1} \otimes a_0, 1_{a_1} \otimes a_0^2, \dots, 1_{a_1} \otimes a_0^{n_0-1} \\ &\quad a_1 \otimes 1_{a_0}, a_1 \otimes a_0, a_1 \otimes a_0^2, \dots, a_1 \otimes a_0^{n_0-1} \\ &\quad \vdots \\ &\quad a_1^{n_1-1} \otimes 1_{a_0}, a_1^{n_1-1} \otimes a_0, a_1^{n_1-1} \otimes a_0^2, \dots, a_1^{n_1-1} \otimes a_0^{n_0-1}\} \end{aligned} \quad (2.2.3)$$

This set of $n_1 n_0$ direct product terms is a linearly independent set and hence can be regarded as a basis of a vector space of dimension $n_1 n_0$ over $GF(p)$. Let the operation of multiplication, denoted by \circ , between two elements from the set (2.2.3) be defined as follows.

$$\begin{aligned}
 (a_1^{i_1} \otimes a_0^{i_0}) \circ (a_1^{j_1} \otimes a_0^{j_0}) &= a_1^{i_1} a_1^{j_1} \otimes a_0^{i_0} a_0^{j_0} \\
 &= (a_1^{i_1+j_1} \text{ modulo } [p; W_1(a_1)]) \otimes (a_0^{i_0+j_0} \text{ modulo } [p; W_0(a_0)])
 \end{aligned}
 \tag{2.2.4}$$

We note here that, multiplication is commutative as the multiplication operation in the two rings are commutative. Further, the multiplication is distributive over addition. Thus,

$$\begin{aligned}
 ((a_1^{i_1} \otimes a_0^{i_0}) + (a_1^{j_1} \otimes a_0^{j_0})) \circ (a_1^{k_1} \otimes a_0^{k_0}) \\
 = (a_1^{i_1+k_1} \otimes a_0^{i_0+k_0}) + (a_1^{j_1+k_1} \otimes a_0^{j_0+k_0})
 \end{aligned}$$

where powers of a_1 and a_0 are reduced to modulo $W_1(a_1)$ and $W_0(a_0)$ respectively. With the multiplication operation defined by (2.2.4) the set of linear combinations of elements from the set (2.2.3) becomes a commutative algebra, called the tensor product of polynomial algebras [61,69], generated by $W_1(a_1)$ and $W_0(a_0)$ over $GF(p)$. We denote this algebra by $P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]$ or alternatively by $\bigotimes_{i=0,1}^T \left\{ P_p^n[W_i(a_i)] \right\}$. Since

we use only the ring property of the tensor product polynomial algebra, we call it tensor product residue class polynomial ring in variables a_1 and a_0 . Tensor product of r residue class polynomial rings $P_p^{n_i}[W_i(a_i)]$; $i = 0, 1, 2, \dots, r-1$, is defined analogously and is denoted by $\bigotimes_{i=0, \dots, r-1}^T P_p^{n_i}[W_i(a_i)]$;

it is the algebra generated by a basis which is the direct product of bases of the r individual rings. The multiplication of elements is carried out as defined by (2.2.4) where powers of a_i are reduced to modulo $[p; W_i(a_i)]$, $i = 0, 1, \dots, r-1$. For the sake of convenience, henceforth we suppress $i = 0, 1, \dots, r-1$ in the notation and the tensor product of r residue class polynomial rings is simply written as $\bigotimes^T P_p^{n_i}[W_i(a_i)]$.

It can be shown that, the tensor product of r residue class polynomial rings generated by $W_{r-1}(a_{r-1})$, ... and $W_0(a_0)$ is isomorphic to a residue class polynomial ring of r -variables $a_{r-1}, a_{r-2}, \dots, a_1, a_0$, where the addition and multiplication operations are carried out modulo $[p; W_{r-1}(a_{r-1}), \dots, W_0(a_0)]$. For the sake of convenience, in what follows we do not make a distinction between the above mentioned isomorphic rings and treat the residue class polynomial ring in more than one variable as appropriate tensor product of residue class polynomial rings. As a consequence, the direct product notation \bigotimes is dropped. Thus, for example, in the tensor product the direct product of identity elements $1_{a_1} \bigotimes 1_{a_0}$ is written simply as 1

and the monomials $1, a_0, \dots, a_0^{n_0-1}, \dots, a_1, a_1 a_0, \dots, a_1 a_0^{n_0-1}, \dots, a_1^{n_1-1} a_0, \dots, a_1^{n_1-1} a_0^{n_0-1}$ are treated as basis elements; however the order in which they are written is maintained.

We note that, when $n_1 = n_0 = 1$, the basis has single element 1, the linear combination of which over $GF(p)$ gives $GF(p)$ itself.

In general consider a tensor product of r residue class polynomial rings given below.

$$P_p^{n_{r-1}}[W_{r-1}(a_{r-1})] \otimes P_p^{n_{r-2}}[W_{r-2}(a_{r-2})] \dots \otimes P_p^{n_0}[W_0(a_0)]$$

From the direct product of bases it is seen that, if

$n_{r-1} = n_{r-2} = \dots = n_1 = 1$, then this ring is isomorphic to

$P_p^{n_0}[W_0(a_0)]$. Thus, residue class polynomial rings in one variable can be regarded as a special case of tensor product of polynomial rings. The tensor product of residue class polynomial rings then become a general class of residue class polynomial rings. In the specific case when $n_i = 1$ for all $i = 0, \dots, r-1$, the tensor product of residue class polynomial ring is isomorphic to $GF(p)$.

Example 2.2.5

Consider the tensor product of residue class polynomial

rings $P_2^2[a_1^2+1]$ and $P_2^2[a_0^2+a_0+1]$ denoted by

$P_2^2[a_1^2+1] \overset{T}{\otimes} P_2^2[a_0^2+a_0+1]$. A basis of $P_2^2[a_0^2+a_0+1]$ is $\{1, a_0\}$.

A basis of $P_2^2[(a_1^2+1)]$ is $\{1, a_1\}$. Basis of

$P_2^2[a_1^2+1] \overset{T}{\otimes} P_2^2[a_0^2+a_0+1]$ is $\{1, a_0, a_1, a_1a_0\}$; the set of all

linear combinations over $GF(2)$ of these elements constitute the

ring $P_2^2[a_1^2+1] \overset{T}{\otimes} P_2^2[a_0^2+a_0+1]$. The addition operation is modulo 2 addition and multiplication operation is modulo

$[2; (a_1^2+1), (a_0^2+a_0+1)]$.

For example consider two elements $(1+a_1a_0)$ and $(1+a_0+a_1a_0)$ in this ring. Their addition is

$(1+a_1a_0) + (1+a_0+a_1a_0) = a_0$; multiplication is

$(1+a_1a_0)(1+a_0+a_1a_0) = (1+a_0+a_1a_0 + a_1a_0 + a_1a_0^2 + a_1^2a_0^2)$ modulo

$[2; a_1^2+1, a_0^2+a_0+1]$

$= 1+a_0+a_1(a_0+1)+(a_0+1)$

$= a_1+a_1a_0$.

*

2.3 ISOMORPHISMS IN RESIDUE CLASS RINGS OF POLYNOMIALS

In this section we present conditions under which residue

class polynomial rings over $GF(p)$ are isomorphic to each other. Specifically the conditions for the following classes of rings to be isomorphic have been obtained: i) local rings, (ii) tensor product of primary rings and (iii) tensor product of polynomial ring and residue class polynomial ring in one variable. Conditions for the semisimple and semilocal rings to be isomorphic are considered in the next section.

To begin with we obtain a condition for two residue class polynomial rings (considered as algebras) to be isomorphic to each other. The result is given for the single variable case. Similar result holds good for the tensor product of residue class polynomial rings.

Theorem 2.3.1

Consider two residue class polynomial rings $P_p^n[W(a)]$ and $P_p^n[W'(b)]$ with their bases $\{1, a, \dots, a^{n-1}\}$ and $\{1, b, \dots, b^{n-1}\}$ respectively. Let there be a one-to-one mapping

$$\phi: a^i \mapsto g^i(b) \text{ modulo } W'(b) ; i = 0, 1, \dots, n-1, \text{ degree } g(b) \leq n-1$$

between the basis of $P_p^n[W(a)]$ and a set of elements

$$\{1, g(b), \dots, g^{n-1}(b)\} \text{ of } P_p^n[W'(b)] \text{ such that the set } \{1, g(b), \dots, g^{n-1}(b)\} \text{ is linearly independent in } P_p^n[W'(b)].$$

If the mapping ϕ further satisfies the following properties :

$$\phi: (\alpha a^i + \beta a^j) \mapsto (\alpha g^i(b) + \beta g^j(b)) \text{ modulo } W'(b); \alpha, \beta \in GF(p)$$

$$\phi: a^i \cdot a^j \text{ modulo } W(a) \mapsto g^i(b) \cdot g^j(b) \text{ modulo } W'(b) \quad (2.3.1)$$

then, ϕ is an isomorphism between $P_p^n[W(a)]$ and $P_p^n[W'(b)]$.

Proof :

The order of the two rings are same and is equal to p^n . Hence, to show that ϕ is an isomorphism between $P_p^n[W(a)]$ and $P_p^n[W'(b)]$, we have to show that ϕ preserves the ring operations and $\text{Ker}\phi = 0$.

Let

$$r_1(a) = \sum_{i=0}^{n-1} r_{1i} a^i, \quad r_{1i} \in \text{GF}(p) \text{ and } r_2(a) = \sum_{i=0}^{n-1} r_{2i} a^i, \\ r_{2i} \in \text{GF}(p)$$

be two elements of $P_p^n[W(a)]$. Under the mapping ϕ let

$$\phi(r_1(a)) = \phi\left(\sum_{i=0}^{n-1} r_{1i} a^i\right) = \sum_{i=0}^{n-1} r_{1i} g^i(b) \text{ modulo } [p; W'(b)] \triangleq r_1'(b)$$

and (2.3.2)

$$\phi(r_2(a)) = \phi\left(\sum_{i=0}^{n-1} r_{2i} a^i\right) = \sum_{i=0}^{n-1} r_{2i} g^i(b) \text{ modulo } [p; W'(b)] \triangleq r_2'(b).$$

Then,

$$\begin{aligned} \phi(r_1(a) + r_2(a)) &= \phi\left(\sum_{i=0}^{n-1} r_{1i} a^i + \sum_{i=0}^{n-1} r_{2i} a^i\right) = \phi\left(\sum_{i=0}^{n-1} (r_{1i} + r_{2i}) a^i\right) \\ &= \sum_{i=0}^{n-1} r_{1i} g^i(b) + \sum_{i=0}^{n-1} r_{2i} g^i(b) \text{ modulo } [p; W'(b)] \\ &= r_1'(b) + r_2'(b) \end{aligned} \quad (2.3.3)$$

Likewise,

$$\begin{aligned}
 \phi(r_1(a) \cdot r_2(a)) &= \phi\left(\sum_{i=0}^{n-1} r_{1i} a^i \sum_{j=0}^{n-1} r_{2j} a^j\right) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} r_{1i} r_{2j} \phi(a^i a^j) \\
 &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} r_{1i} r_{2j} (g^i(b) \cdot g^j(b)) = \sum_{i=0}^{n-1} r_{1i} g^i(b) \cdot \\
 &\quad \cdot \sum_{j=0}^{n-1} r_{2j} g^j(b) \text{ modulo}[p; W'(b)] \\
 &= r_1'(b) \cdot r_2'(b). \tag{2.3.4}
 \end{aligned}$$

Thus, ϕ preserves ring operations.

Since the set $\{1, g(b), \dots, g^{n-1}(b)\}$ modulo $[p; W'(b)]$ is linearly independent in $P_p^n[W'(b)]$, $\sum_{i=0}^{n-1} r_{1i} g^i(b) = 0$ implies $r_{1i} = 0$, $i = 0, 1, \dots, n-1$. Hence only $0 \in P_p^n[W(a)]$ is mapped to $0 \in P_p^n[W'(b)]$ that is $\text{Ker } \phi = 0$.

Thus, $\phi: P_p^n[W(a)] \rightarrow P_p^n[W'(b)]$ is an isomorphism. $\tag{2.3.5}$

For the case when $W(a)$ and $W'(b)$ are distinct irreducible polynomials of degree n , $P_p^n[W(a)]$ and $P_p^n[W'(b)]$ are isomorphic finite fields of order p^n as given in [18]. *

Example 2.3.1

Consider finite fields generated by $W(a) = a^3 + a + 1$ and $W'(b) = b^3 + b^2 + 1$ over $\text{GF}(2)$. The set $\{1, a, a^2\}$ constitutes a basis of $P_p^n[W(a)]$ and $\{1, b, b^2\}$ constitutes a basis of $P_p^n[W'(b)]$. Let $\phi: a \rightarrow (1+b) = g(b)$ be a one-to-one mapping between basis

of $P_p^n[W(a)]$ and set of elements of $P_p^n[W'(b)]$. We note that $\{1, 1+b, 1+b^2\}$ constitutes a linearly independent set in $P_p^n[W'(b)]$, and hence constitutes another basis. Further, ϕ satisfies the following conditions.

$$\phi: (\alpha a^i + \beta a^j) \text{ modulo } [2; W(a)] \mapsto (\alpha g^i(b) + \beta g^j(b)) \\ \text{modulo } [2; W'(b)]$$

$$\text{and } \phi: a^i \cdot a^j \text{ modulo } [2; W(a)] \mapsto g^i(b) \cdot g^j(b) \text{ modulo } [2; W'(b)].$$

Therefore from Theorem 2.3.1 $\phi: a \mapsto (1+b)$ is an isomorphism between $P_p^n[W(a)]$ and $P_p^n[W'(b)]$ both of which are finite fields of order 2^3 .

The correspondence between the elements is given below.

$$a^3 = (1+a) \neq b; \quad a^4 = (a+a^2) \neq b+b^2 = b^6;$$

$$a^5 = (1+a+a^2) \neq (1+b+b^2) = b^4; \quad a^6 = 1+a^2 \neq b^2;$$

$$a^7 = 1 \neq b^7 = 1.$$

*

We now state and prove the converse of Theorem 2.3.1.

Theorem 2.3.2

Consider two isomorphic residue class polynomial rings $P_p^n[W(a)]$ and $P_p^n[W'(b)]$ with $\{1, a, \dots, a^{n-1}\}$ and $\{1, b, \dots, b^{n-1}\}$ respectively, as their basis. If the isomorphism ϕ between these two rings is given by

$$\phi: a^i \mapsto g^i(b) \text{ modulo } [p; W'(b)]; \quad i = 0, 1, \dots, n-1. \quad (2.3.6)$$

where $g(b) \in P_p^n[W'(b)]$, then the set $\{1, g(b), \dots,$

$g^{n-1}(b)\}$ modulo $[p; W'(b)]$ is linearly independent and hence constitutes another basis of $P_p^n[W'(b)]$.

Proof

$$\text{Let } r(a) = \sum_{i=0}^{n-1} r_i a^i ; \quad r_i \in GF(p) \quad (2.3.7)$$

be an element of $P_p^n[W(a)]$. Under the isomorphism ϕ , we have

$$\phi: (r(a)) \rightarrow \sum_{i=0}^{n-1} r_i g^i(b) \text{ modulo } [p; W'(b)]. \quad (2.3.8)$$

Further, $r(a) = 0$ iff $r_i = 0$,

Since ϕ is an isomorphism $\text{Ker } \phi = 0$. Hence, only $0 \in P_p^n[W(a)]$ is mapped to $0 \in P_p^n[W'(b)]$. Thus,

$$\sum_{i=0}^{n-1} r_i g^i(b) \text{ modulo } [p; W'(b)] = 0 \text{ iff } r_i = 0 \quad (2.3.9)$$

Hence $\{1, g(b), \dots, g^{n-1}(b)\}$ modulo $[p; W'(b)]$ is a linearly independent set.

*

2.3.1 Isomorphisms in Local $P_p^n[W(a)]$

We now use the foregoing theorems in conjunction with the result that finite fields generated by the irreducible polynomials of same degree are isomorphic to each other, to obtain the conditions for the local rings to be isomorphic to each other.

Lemma 2.3.1

If ϕ is an isomorphism between two finite fields $P_p^n[W(a)]$ and $P_p^n[W'(b)]$ of order p^n generated by n th degree distinct irreducible polynomials $W(a)$ and $W'(b)$ respectively, then the local rings $P_p^{hn}[W^h(a)]$ and $P_p^{hn}[W'^h(b)]$ of order p^{hn} generated by $W^h(a)$ and $W'^h(b)$ respectively are also isomorphic with ϕ as the isomorphism between them.

Proof

The lemma is proved using the result of Theorem 2.3.2. For $h = 1$ we have $P_p^n[W(a)] \cong P_p^n[W'(b)]$. While, $\{1, a, \dots, a^{n-1}\}$ is a basis of $P_p^n[W(a)]$, $\{1, b, \dots, b^{n-1}\}$ is a basis of $P_p^n[W'(b)]$. If ϕ denotes the isomorphism $\phi : a^i \rightarrow g^i(b)$ modulo $[p; W'(b)]$, $i = 0, 1, 2, \dots, n-1$ between $P_p^n[W(a)]$ and $P_p^n[W'(b)]$, then by Theorem 2.3.2 the set $\{1, g(b), \dots, g^{n-1}(b)\}$ modulo $[p; W'(b)]$, is linearly independent.

Consider the following set of hn elements in $P_p^{hn}[W(a)]$

$$\{1, a, a^2, \dots, a^{n-1}, W(a), aW(a) \dots a^{n-1}W(a), W^2(a) \dots a^{n-1}W^2(a),$$

$$W^{h-1}(a), \dots, a^{n-1}W^{h-1}(a)\} \quad (2.3.10)$$

The set (2.3.10) is a linearly independent set of hn elements and hence constitutes a basis of $P_p^{hn}[W^h(a)]$.

Using the correspondence $\phi : a \rightarrow g(b)$, we get the following set of hn elements in $P_p^{hn}[W'^h(b)]$.

$$\{1, g(b), \dots, g^{n-1}(b), W'(b), \dots, g^{n-1}(b), W'(b), \dots$$

$$W'^{h-1}(b), \dots, g^{n-1}(b), W'^{(h-1)}(b)\} \text{ modulo } [p; W'(b)] \quad (2.3.11)$$

Since the set $\{1, g(b), \dots, g^{n-1}(b)\} \text{ modulo } [p; W'(b)]$ is a linearly independent set of n elements, (2.3.11) is also a linearly independent set of hn elements in $P_p^{hn}[W'^h(b)]$ and hence constitutes a basis of $P_p^{hn}[W'^h(b)]$. It follows that \emptyset establishes a one-to-one correspondence between (2.3.10) and (2.3.11). Further, it can be verified that \emptyset satisfies the conditions of Theorem 2.3.1. Hence, the local rings $P_p^{hn}[W^h(a)]$ and $P_p^{hn}[W'^h(b)]$ are isomorphic and \emptyset is the isomorphism between them.

*

Example 2.3.2

Consider the local rings $P_2^6[(a^3+a+1)^2]$ and $P_2^6[(b^3+b^2+1)^2]$. A basis of $P_2^6[(a^3+a+1)^2]$ is $\{1, a, a^2, (1+a+a^3), a(1+a+a^3), a^2(1+a+a^3)\}$.

Let $\emptyset : a \mapsto (1+b)$, then $\{1, (1+b), (1+b^2), (1+b^2+b^3), (1+b)(1+b^2+b^3), (1+b^2)(1+b^2+b^3)\}$ constitutes a basis of $P_2^6[(b^3+b^2+1)^2]$. Further, \emptyset also satisfies conditions given in Theorem 2.3.1 and hence establishes an isomorphism between the two given local rings.

*

2.3.2 Isomorphisms in $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$

The results of the Subsection 2.3.1 can be used to obtain isomorphisms in the tensor products of primary residue class polynomial rings. Consider $P_p^{n_0}[W_0(a_0)]$ and $P_p^{n_1}[W_1(a_1)]$, degree of $W_i(a_i)$ being n_i ; $i = 0, 1$. We first prove the following lemma concerning the isomorphisms between the tensor products of the polynomial rings generated by $W_0(a_0)$ and $W_1(a_1)$.

Lemma 2.3.2

$P_p^{n_0}[W_0(a_0)] \bigotimes^T P_p^{n_1}[W_1(a_1)]$ is isomorphic to

$$P_p^{n_1}[W_1(a_1)] \bigotimes^T P_p^{n_0}[W_0(a_0)]$$

Proof

The lemma is proved by establishing one-to-one mapping \emptyset between the basis of the two tensor product residue class polynomial rings which satisfies the conditions of Theorem 2.3.1.

Consider $P_p^{n_0}[W_0(a_0)] \bigotimes^T P_p^{n_1}[W_1(a_1)]$

A basis for this ring is

$$\begin{aligned} & 1_{a_0} \otimes 1_{a_1}, 1_{a_0} \otimes a_1, 1_{a_0} \otimes a_1^2 \dots 1_{a_0} \otimes a_1^{n_1-1} \\ & a_0 \otimes 1_{a_1}, a_0 \otimes a_1, a_0 \otimes a_1^2, \dots a_0 \otimes a_1^{n_1-1} \\ & \vdots \\ & a_0^{n_0-1} \otimes 1_{a_1}, a_0^{n_0-1} \otimes a_1, \dots a_0^{n_0-1} \otimes a_1^{n_1-1} \quad (2.3.12) \end{aligned}$$

Likewise a basis for $P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)]$ is

$$\begin{array}{cccc}
 1_{a_1} \otimes 1_{a_0}, & 1_{a_1} \otimes a_0, & 1_{a_1} \otimes a_0^2 \dots & 1_{a_1} \otimes a_0^{n_0-1} \\
 a_1 \otimes 1_{a_0}, & a_1 \otimes a_0, & a_1 \otimes a_0^2 \dots & a_1 \otimes a_0^{n_0-1} \\
 \vdots & & & \vdots \\
 a_1^{n_1-1} \otimes 1_{a_0}, & a_1^{n_1-1} \otimes a_0, & a_1^{n_1-1} \otimes a_0^2 \dots & a_1^{n_1-1} \otimes a_0^{n_0-1}
 \end{array}
 \quad (2.3.13)$$

There is a one-to-one mapping

$$\phi: a_0^{i_0} \otimes a_1^{i_1} \rightarrow a_1^{i_1} \otimes a_0^{i_0} \quad 0 \leq i_1 \leq n_1-1; 0 \leq i_0 \leq n_0-1;$$

$$\begin{array}{l}
 \text{where,} \quad a_0^0 \triangleq 1_{a_0} \\
 \text{and} \quad a_1^0 \triangleq 1_{a_1}
 \end{array}$$

between the basis elements (2.3.12) and (2.3.13)

$$\text{Further, } \phi: (\alpha a_0^{i_0} \otimes a_1^{i_1} + \beta a_0^{j_0} \otimes a_1^{j_1}) \rightarrow (\alpha a_1^{i_1} \otimes a_0^{i_0} + \beta a_1^{j_1} \otimes a_0^{j_0})$$

$$\phi: (a_0^{i_0} \otimes a_1^{i_1})(a_0^{j_0} \otimes a_1^{j_1}) \rightarrow (a_1^{i_1} \otimes a_0^{i_0})(a_1^{j_1} \otimes a_0^{j_0})$$

$$\text{that is } \phi: (a_0^{i_0+j_0} \text{ modulo } [p; W_0(a_0)]) \otimes (a_1^{i_1+j_1} \text{ modulo } [p; W_1(a_1)])$$

$$\rightarrow (a_1^{i_1+j_1} \text{ modulo } p; W_1(a_1)) \otimes (a_0^{i_0+j_0} \text{ modulo } p; W_0(a_0))$$

Thus, ϕ satisfies the conditions of Theorem 2.3.1 and by

Theorem 2.3.1 the two tensor product rings are isomorphic to each other.

In the next Lemma we consider isomorphism between rings which are tensor product of local rings.

Lemma 2.3.3

$$\text{Let } P_p^{h_0 n_0}[W_0^{h_0}(a_0)] \simeq P_p^{h_0 n_0}[W_0^{h_0}(b_0)] \quad (2.3.14)$$

$$P_p^{h_1 n_1}[W_1^{h_1}(a_1)] \simeq P_p^{h_1 n_1}[W_1^{h_1}(b_1)] \quad (2.3.15)$$

where $W_0(a_0)$ and $W_0(b_0)$ are distinct irreducible polynomials of degree n_0 and $W_1(a_1)$ and $W_1(b_1)$ are distinct irreducible polynomials of degree n_1 . Then the tensor products

$$P_p^{h_0 n_0}[W_0^{h_0}(a_0)] \otimes P_p^{h_1 n_1}[W_1^{h_1}(a_1)] \quad (2.3.16)$$

and

$$P_p^{h_0 n_0}[W_0^{h_0}(b_0)] \otimes P_p^{h_1 n_1}[W_1^{h_1}(b_1)] \quad (2.3.17)$$

are isomorphic.

Proof

There is a one-to-one mapping ϕ between the elements of the bases of (2.3.16) and (2.3.17) which also satisfies the conditions given in Theorem 2.3.1. From the results of Theorem (2.3.1), ϕ is an isomorphism between the tensor product residue class polynomial rings which proves the lemma.

*

Example 2.3.3

Consider the following tensor products of rings

$$P_2^4[(a_1^2+a_1+1)^2] \overset{T}{\otimes} P_2^3[b_1^3+b_1+1] \quad (2.3.18)$$

and

$$P_2^4[(a_2^2+a_2+1)^2] \overset{T}{\otimes} P_2^3[b_2^3+b_2^2+1] \quad (2.3.19)$$

We have seen that

$$P_2^3[b_1^3+b_1+1] \simeq P_2^3[b_2^3+b_2^2+1]$$

A basis of tensor product ring (2.3.18) is

$$\{1, b_1, b_1^2, a_1, a_1 b_1, a_1 b_1^2, a_1^2, a_1^2 b_1, a_1^2 b_1^2, a_1^3, a_1^3 b_1, a_1^3 b_1^2\} \quad (2.3.20)$$

With the one-to-one mapping $\emptyset: b_1 \longrightarrow (b_2+1)$ the basis given by Equation (2.3.20) is mapped to a basis

$$\{1, (b_2+1), (b_2+1)^2, a_2, a_2(b_2+1), a_2(b_2+1)^2, a_2^2, a_2^2(b_2+1), a_2^2(b_2+1)^2, \\ a_2^3, a_2^3(b_2+1), a_2^3(b_2+1)^2\},$$

since \emptyset satisfies the conditions given in Theorem 2.3.1, tensor product rings given by Expressions (2.3.18) and (2.3.19) are isomorphic to each other.

*

We next consider the isomorphisms between residue class polynomial ring and tensor product of residue class polynomial rings.

2.3.3 Isomorphisms between $P_p^n[W(a)]$ and $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$

Consider the tensor product of residue class polynomial rings generated by polynomials $W_0(a_0)$ and $W_1(a_1)$ of degree n_0 and n_1 respectively over $GF(p)$. This ring is denoted by $P_p^{n_1}[W_1(a_1)] \bigotimes^T P_p^{n_0}[W_0(a_0)]$. Since this is also an algebra of dimension $n = n_1 n_0$, one set of basis vector is

$$\{1, a_0, a_0^2, \dots, a_0^{n_0-1}, a_1, a_1 a_0, a_1 a_0^2, \dots, a_1 a_0^{n_0-1}, \dots, a_1^{n_1-1}, a_1^{n_1-1} a_0, a_1^{n_1-1} a_0^2, \dots, a_1^{n_1-1} a_0^{n_0-1}\} \quad (2.3.21)$$

To check whether the tensor product ring is isomorphic to a residue class polynomial ring in one variable, we consider the set

$$\{1, a_1 a_0, a_1^2 a_0^2, \dots, a_1^{n-1} a_0^{n-1}\} \text{ modulo } [W_1(a_1), W_0(a_0)] \quad (2.3.22)$$

of powers $a_1^j a_0^j$ modulo $[W_1(a_1), W_0(a_0)]$; $0 \leq j < n$ $n = n_1 n_0$, i.e. for $h_i \geq n_i, a_i^{h_i}$ is a linear combination of powers of a_i whose degree is less than n_i ; $i = 0, 1$. We check for the linear dependency in (2.3.22). If the n terms are linearly independent then the set (2.3.22) can be regarded as a basis of residue class polynomial ring in two variables.

Now with the map $\phi: a_1 a_0 \rightarrow a$ we obtain a new linearly independent set

$$\{1, a, \dots, a^{n-1}\} \text{ modulo } [p; W(a)] \quad (2.3.23)$$

If \emptyset also satisfies the conditions given in Theorem 2.3.1, then the residue class polynomial ring in two variables with (2.3.22) as basis is isomorphic to the residue class polynomial ring in one variable with (2.3.23) as basis. Because of the transitivity property of isomorphisms tensor product of two residue class polynomial rings is then isomorphic to residue class polynomial ring in one variable. However, determination of modulus polynomial $W(a)$ is not straight forward.

The isomorphisms are illustrated in Figure 2.3.1.

If the elements in (2.3.22) are linearly dependent, tensor product residue class polynomial ring $P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]$ is not isomorphic to any residue class polynomial ring generated by a polynomial in one variable. We have thus proved the following theorem.

Theorem 2.3.3

The necessary condition for the tensor product of residue class polynomial rings generated by $W_1(a_1)$ and $W_0(a_0)$ to be isomorphic to a residue class polynomial rings generated by a polynomial of degree n in one variable is that the elements in the set

$$\{1, a_1 a_0, a_1^2 a_0^2, \dots, a_1^{n-1} a_0^{n-1}\} \text{ modulo } [p; W_1(a_1), W_0(a_0)]$$

are linearly independent.

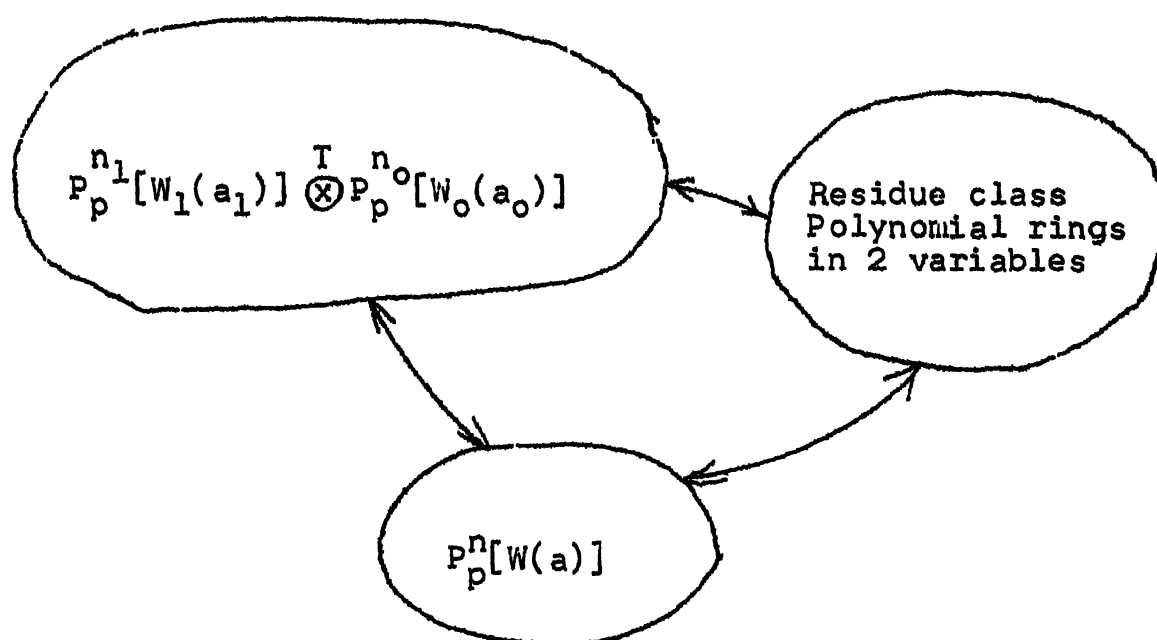


Figure 2.3.1 Isomorphisms between tensor product of residue class polynomial rings, and residue class polynomial rings

Example 2.3.4

Consider the tensor product of a local ring and finite field $P_2^2[a_1^2+1] \otimes P_2^2[(a_0^2+a_0+1)]$. The set $\{1, a_1a_0, a_1^2a_0^2, a_1^3a_0^3\}$, computed modulo $[2, (a_1^2+1), (a_0^2+a_0+1)]$ is $\{1, a_1a_0, (1+a_0), a_1\}$ which is linearly independent over $GF(2)$. Let $\phi: a_1a_0 \rightarrow a$, further if ϕ satisfies the conditions of Theorem 2.3.1, then the tensor product of residue class polynomial ring $P_2^2[a_1^2+1] \otimes P_2^2[a_0^2+a_0+1]$ may be isomorphic to a residue class polynomial ring generated by a polynomial in one variable. With the mapping $a_1a_0 \rightarrow a$ we have $1 \rightarrow 1$, $(1+a_0) \rightarrow a^2$, $a_1 \rightarrow a^3$. To check whether ϕ satisfies the conditions given in Theorem 2.3.1 we must know $W(a)$.

In general the determination of $W(a)$ is not straight forward. For simple cases as in this example it can be determined in the following manner.

Using the one-to-one correspondence between (a_1a_0) and 'a' we write $W_0(a_0)$ in terms of 'a'. Let this new polynomial be $W'_0(a)$. Similarly we write $W_1(a_1)$ in terms of 'a' giving rise to a polynomial $W'_1(a)$. $W(a)$ is chosen such that it is the least degree monic polynomial satisfying

$$W'_0(a) = 0 \text{ modulo } [2, W(a)] \quad (2.3.24)$$

$$W'_1(a) = 0 \text{ modulo } [2, W(a)]$$

In this example we have

$$W_0(a_0) = (a_0^2 + a_0 + 1) \approx (a^4 + 1) + (a^2 + 1) + 1 = (a^4 + a^2 + 1) = W'_0(a)$$

and

$$W_1(a_1) = (a_1^2 + 1) \approx (a^6 + 1) = W'_1(a)$$

Here $W(a) = (a^4 + a^2 + 1)$ satisfies the condition (2.3.24)

i.e.,

$$W'_0(a) = (a^4 + a^2 + 1) = 0 \text{ modulo } [2, a^4 + a^2 + 1]$$

$$\text{and } W'_1(a) = (a^6 + 1) = 0 \text{ modulo } [2, a^4 + a^2 + 1].$$

It can be verified now that \emptyset satisfies the conditions given in Theorem 2.3.1.

$$\text{Hence, } P_2^2[a_1^2 + 1] \overset{T}{\underset{(X)}{\otimes}} P_2^2[a_0^2 + a_0 + 1] \approx P_2^4[a^4 + a^2 + 1].$$

*

Example 2.3.5

Consider the tensor product of two local rings

$$P_2^2[(a_1^2 + 1)] \overset{T}{\underset{(X)}{\otimes}} P_2^2[(a_0^2 + 1)]. \text{ The set } \{1, a_1 a_0, a_1^2 a_0^2, a_1^3 a_0^3\}$$

computed modulo $[2; (a_1^2 + 1), (a_0^2 + 1)]$ is

$\{1, a_1 a_0, 1, a_1 a_0\}$ which is a linearly dependent set.

Hence, $P_2^2[(a_1^2 + 1)] \overset{T}{\underset{(X)}{\otimes}} P_2^2[a_0^2 + 1]$ is not isomorphic to a residue class polynomial ring generated by a polynomial in one variable over $GF(2)$.

*

We have seen that $P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)]$ is isomorphic to a $P_p^n[W(a)]$ iff the set given by (2.3.22) is a linearly independent set. An alternative test to check whether the tensor product ring is isomorphic to a $P_p^n[W(a)]$ is obtained below, where it is not required to write all the n terms in (2.3.22) and reduce them modulo $[p, W_1(a), W_0(a_0)]$.

If T_i is the least integer such that $W_i(a_i)$ divides $(a_i^{T_i} - 1)$, then T_i is called the period (exponent) of $W_i(a_i)$ $a_i^{T_i} = 1$ modulo $[p; W_i(a_i)]$, $i = 0, 1$. Let $T = \text{lcm}(T_0, T_1)$. A sufficient condition for the set given by (2.3.22) to be linearly dependent can be obtained in terms of T and $n = n_1 n_0$, which also leads to the condition for $P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)]$ not to be isomorphic to a $P_p^n[W(a)]$. Towards this end we prove the following theorem.

Theorem 2.3.4

If $T < n$ the set $\{1, a_1 a_0, \dots, a_1^{n-1} a_0^{n-1}\}$ is a linearly dependent set and hence the tensor product ring $P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)]$ is not isomorphic to $P_p^n[W(a)]$.

Proof

T is the lcm of the periods of $W_1(a_1)$ and $W_0(a_0)$.

Hence, $a_1^T = 1$ modulo $[p; W_1(a_1)]$

$$a_0^T = 1 \text{ modulo } [p; W_0(a_0)]$$

and $a_1^T a_0^T = 1$ modulo $[p; W_1(a_1), W_0(a_0)]$.

Consider the set $\{1, a_1 a_0, \dots, a_1^{n-1} a_0^{n-1}\}$

Since $T < n$ in the above set 1 occurs at least twice.
Hence the set is linearly dependent set, and from the
result of Theorem 2.3.3 the tensor product ring is not
isomorphic to $P_p^n[W(a)]$. *

Example 2.3.6

Consider the tensor product of two rings one of which
is a semisimple ring and the other is a field;

$$P_2^3[(a_1^3+1)] \overset{T}{\otimes} P_2^2[a_0^2+a_0+1] \quad n = n_1 n_0 = 6$$

Period of $a_0^2+a_0+1$ is 3

Period of a_1^3+1 is 3

lcm of periods is $3 < 6$

Hence $P_2^3[a_1^3+1] \overset{T}{\otimes} P_2^2[a_0^2+a_0+1]$ is not isomorphic to any
 $P_2^6[W(a)]$; residue class polynomial ring in one variable.*

Example 2.3.7

Consider the tensor product of two rings one of which
is semisimple ring and the other is a local ring

$$P_2^3[a_1^3+1] \overset{T}{\otimes} P_2^2[a_0^2+1], \quad n = n_1 n_0 = 6$$

Period of (a_0^2+1) is 2

Period of (a_1^3+1) is 3

lcm of periods is $n = 6$.

$P_2^3[a_1^3+1] \overset{T}{\otimes} P_2^2[a_0^2+1]$ is isomorphic to a residue class polynomial ring. A basis of the ring is

$$\{1, a_1 a_0, a_1^2 a_0^2, \dots, a_1^5 a_0^5\} \text{ modulo } [2; W_1(a_1), W_0(a_0)]$$

$$= \{1, a_1 a_0, a_1^2, a_0, a_1, \dots, a_1^2 a_0\} \quad (2.3.25)$$

With the mapping $a_1 a_0 \rightleftharpoons a$
we have a corresponding set

$$\{1, a, a^2, a^3, a^4, a^5\} \quad (2.3.26)$$

which is linearly independent and hence constitutes a basis.

Writing $W_0(a_0)$ and $W_1(a_1)$ in terms of new basis we get

$$W_0(a_0) = (a_0^2+1) \rightleftharpoons (a^6+1) = W'_0(a)$$

$$W_1(a_1) = (a_1^3+1) \rightleftharpoons (a^6+1) = W'_1(a) .$$

Hence tensor product of the given semisimple and local ring is isomorphic to semilocal ring $P_2^6[a^6+1]$.

*

The results of the Theorems 2.3.3 and 2.3.4 can be extended to the case $r > 2$. For example, consider the tensor product of three rings $P_p^{n_0}[W_0(a_0)]$, $P_p^{n_1}[W_1(a_1)]$, and $P_p^{n_2}[W_2(a_2)]$ where $n = n_2 n_1 n_0$. If the set

$$\{1, a_2 a_1 a_0, a_2^2 a_1^2 a_0^2, \dots, a_2^{n-1} a_1^{n-1} a_0^{n-1}\} \text{ modulo } [p, W_2(a_2),$$

$$W_1(a_1), W_0(a_0)] \quad (2.2.27)$$

is a linearly independent set, then the tensor product of the two rings is isomorphic to a residue class polynomial ring in one variable. If the set (2.3.27) is a linearly dependent set but the set,

$$\{1, a_i a_j, a_i^2 a_j^2, \dots, a_i^{n'-1} a_j^{n'-1}\}, \quad (2.2.28)$$

where all the elements are computed modulo $W_i(a_i), W_j(a_j)$,
 $n' = n_i n_j$.

$i, j = 0, 1, 2, ; i \neq j$ is a linearly independent set then the tensor product of the given three polynomial rings is isomorphic to another tensor product of two polynomial rings.

If $T = \text{lcm}(T_2, T_1, T_0)$ where T_i is the period of $W_i(a_i)$ $i = 0, 1, 2$, then $T < n_2 n_1 n_0$ implies that the set (2.3.27) is linearly dependent and hence not isomorphic to $P_p^n[W(a)]$.

Thus a tensor product of j residue class polynomial rings may be isomorphic to a residue class polynomial ring in one variable or a tensor product of $(j-1)$ or less residue class polynomial rings in one variable.

Theorems 2.3.1 and 2.3.2 can also be used to obtain specific conditions for isomorphisms in semisimple and semilocal rings. However, in practice to obtain the desired isomorphism is quite involved. In the next section we consider decomposition of semilocal and semisimple rings into primary rings and use these decomposition results to obtain conditions for isomorphisms in semisimple and semilocal rings in terms of results on isomorphisms in finite fields and local rings.

2.4 DECOMPOSITION OF RESIDUE CLASS RINGS OF POLYNOMIALS

We have seen in Section 2.2 that $P_p^n[W(a)]$ can be classified as finite fields local rings, semisimple rings, or semilocal rings depending on the prime factorisation of the modulus polynomial $W(a)$. This classification has been summarised in Table 2.2.1.

A semisimple or semilocal $P_p^n[W(a)]$ can be expressed as internal direct sum of ideals isomorphic to primary rings or alternatively can be expressed as a ring isomorphic to external direct sum of smaller primary rings. This provides decomposition of $P_p^n[W(a)]$ into primary rings, which are either finite fields or local rings. In this chapter decomposition of $P_p^n[W(a)]$ in combination with ring isomorphisms will be utilised in Section 2.5 to enumerate nonisomorphic residue class polynomial rings $P_p^n[W(a)]$, of a given order. In later chapters decomposition of $P_p^n[W(a)]$ is utilised for (i) obtaining conditions for nilpotence of characteristic matrix A , (ii) computation of period of characteristic matrix A and (iii) decomposition of sequences over $P_p^n[W(a)]$ into orthogonal sequences.

Decomposition of tensor product of residue class polynomial rings is carried out making use of the distributive property of the tensor product over direct sum decomposition [73].

2.4.1 Decomposition of $P_p^n[W(a)]$

Decomposition of the ring $P_p^n[W(a)]$ is carried out on lines similar to the decomposition of Z_m ; the role of irreducible polynomials and their powers in the case of $P_p^n[W(a)]$ is similar to the role of prime numbers and their powers in the case of Z_m . Thus if m_1, m_2, \dots, m_k are pairwise relatively prime factors of m , then Z_m is isomorphic to $Z_{m_1} \oplus Z_{m_2} \oplus \dots \oplus Z_{m_k}$ [64]. However, it may be noted that in general Z_m is not isomorphic to $P_p^n[W(a)]$ except for the case $Z_p = P_p^1[W(a)] = GF(p)$. (The comparison of Z_m and $P_p^n[W(a)]$ is summarised in Appendix H).

The internal direct sum decomposition is considered first.

Let,

$$W(a) = \prod_{i=1}^{\nu} W_i^{h_i}(a) \quad (2.4.1)$$

where, $W_i(a)$; $i = 1, 2, \dots, \nu$ are the distinct irreducible factors of $W(a)$ over $GF(p)$.

$$\text{Let } \overline{W_j^{h_j}(a)} = \prod_{\substack{i=1 \\ i \neq j}}^{\nu} W_i^{h_i}(a)$$

Then $\overline{W_j^{h_j}(a)}$; $j = 1, 2, \dots, \nu$ are pairwise relatively prime.

There exists unique elements $b_1(a), b_2(a), \dots, b_{\nu}(a)$ in $P_p^n[W(a)]$ such that,

$$\overline{W_1^{h_1}(a)} b_1(a) + \overline{W_2^{h_2}(a)} b_2(a) + \dots + \overline{W_{\nu}^{h_{\nu}}(a)} b_{\nu}(a) = 1 \text{ modulo } [p; W(a)]$$

Let $\overline{W_i^{h_i}}(a) \triangleq e_i(a)$; the set

$$\{e_1(a), e_2(a), \dots, e_\nu(a)\} \quad (2.4.2)$$

is such that $e_i(a), e_j(a), i \neq j$, is a multiple of $W(a)$ hence,

$$e_i(a) \cdot e_j(a) = 0 \text{ modulo } [p; W(a)]; i \neq j \quad (2.4.3)$$

$$e_1(a) + e_2(a) + \dots + e_\nu(a) = 1 \text{ modulo } [p; W(a)] \quad (2.4.4)$$

and

$$e_i^2(a) = e_i(a) \text{ modulo } [p; W(a)] \quad (2.4.5)$$

Equation (2.4.5) implies that $e_i(a)$ is an idempotent in $P_p^n[W(a)]$. From Expressions (2.4.3), (2.4.4) and (2.4.5), it follows that the set (2.4.2) forms a set of mutually orthogonal idempotents.

Let J_i be the ideal generated by orthogonal idempotent $e_i(a)$ in $P_p^n[W(a)]$, that is, $J_i = \langle e_i(a) \rangle$; $i = 1, 2, \dots, \nu$.

Every element $r_i(a) \in J_i$ and $r_j(a) \in J_j$ are multiples of $e_i(a)$ and $e_j(a)$ respectively. Since $e_i(a) \cdot e_j(a) = 0 \text{ modulo } [p; W(a)]; i \neq j$, $r_i(a) \cdot r_j(a) = 0 \text{ modulo } [p; W(a)]$. Thus, ideals J_1, J_2, \dots, J_ν are such that elements from different ideals annihilate each other. We call these ideals orthogonal ideals. In what follows we will say that the elements drawn from orthogonal ideals J_i and J_j , $i \neq j$ are orthogonal to each other. It should

be noted that this notion of orthogonality is not in the usual inner product sense.

Thus J_1, J_2, \dots, J_ν have the property that

$$J_i \cap (J_1 + J_2 + \dots + J_{i-1} + J_{i+1} + \dots + J_\nu) = 0 \text{ modulo } [p; W(a)]$$

$$i = 1, 2, \dots, \nu \quad (2.4.6)$$

and for any $r(a) \in P_p^n[W(a)]$, $r(a) = 1 \cdot r(a) = (e_1(a) + \dots$

$$e_\nu(a)) r(a) \text{ modulo } [p; W(a)]$$

$$= r_1(a) + r_2(a) + \dots + r_\nu(a) \text{ modulo } [p; W(a)],$$

where $r_i(a) = r(a) \cdot e_i(a) \in J_i$.

For a given $r(a)$ the unique set of orthogonal elements $r_1(a)$, $r_2(a)$, \dots , $r_\nu(a)$ constitutes the internal direct sum components of $r(a)$. This leads to the notion of decomposition of ring $P_p^n[W(a)]$ into internal direct sum of orthogonal ideals.

Thus,

$$P_p^n[W(a)] = J_1 + J_2 + \dots + J_\nu \text{ modulo } [p; W(a)]$$

If $r(a)$ is a factor of $W(a)$, then it is a zero divisor, that is there is a $q(a)$ such that $r(a) \cdot q(a) = W(a) = 0 \text{ modulo } [p; W(a)]$.

Since $e_i(a) = \overline{W_i^{h_i}}(a) b_i(a)$, at least one $e_i(a)$ is a multiple of $q(a)$ and hence $e_i(a) \cdot r(a) = 0 \text{ modulo } [p; W(a)]$. As a consequence if $r(a)$ is a zero divisor, in its internal direct sum component at least one component is zero. The converse is also true.

When $W(a)$ is as given by Equation (2.4.1), $\langle W_i(a) \rangle$, $i = 1, 2, \dots, \nu$ are the maximal ideals in $P_p^n[W(a)]$. Hence in this case $P_p^n[W(a)]$ is a semilocal ring. Elements which are multiples of $\prod_{i=1}^{\nu} W_i(a)$ are nilpotent in $P_p^n[W(a)]$. When $h_i = 1$ $\forall i = 1, 2, \dots, \nu$, ideal J_i is generated by $e_i(a)$ which is a multiple of $\prod_{j=1, j \neq i}^{\nu} W_j(a)$; Hence J_i $i = 1, 2, \dots, \nu$ are not only orthogonal ideals but in addition are also simple ideals. Any nonzero element in J_i will not have $W_i(a)$ as a factor $i = 1, 2, \dots, \nu$. Since any nilpotent element must be a multiple of $\prod_{i=1}^{\nu} W_i(a)$, zero is the only nilpotent element. Hence, when $h_i = 1$, i , $P_p^n[W(a)]$ is semisimple. It is equal to the internal direct sum of simple ideals.

Decomposition of ring $P_p^n[W(a)]$ into internal direct sum is used in the decomposition of $P_p^n[W(a)]$ -LSS and in the computation of period of characteristic matrix A in Chapter 3, enumeration of state cycles in Chapter 4 and computation of minimum distance of cyclic codes over semisimple ring in Chapter 5.

We now take up the external direct sum of $P_p^n[W(a)]$. $W(a)$ given by Expression (2.4.1) is such that $W_i^{h_i}(a)$; $i = 1, 2, \dots, \nu$ are pairwise relatively prime. From the Chinese remainder theorem (Appendix E) for polynomials over $GF(p)$, there is a one-to-one correspondence between elements of $P_p^n[W(a)]$ and ν -tuples.

Suppose $r(a) \in P_p^n[W(a)]$, then

$$r(a) \approx (\tilde{r}_1(a), \tilde{r}_2(a), \dots, \tilde{r}_\nu(a)), \quad (2.4.7)$$

where $\tilde{r}_i(a) = r(a) \text{ modulo } [p; W_i^{h_i}(a)]$; is element of local ring $P_p^{h_i n_i}[W_i^{h_i}(a)]$; $i = 1, 2, \dots, \nu$ and it can be shown that

$$r_i(a) = \tilde{r}_i(a) \cdot e_i(a) \text{ modulo } [p; W(a)] \quad (2.4.8)$$

and

$$\tilde{r}_i(a) = r_i(a) \text{ modulo } [p; W_i^{h_i}(a)] \quad (2.4.9)$$

The internal direct sum decomposition of $r(a)$ that is

$$r(a) = r_1(a) + r_2(a) + \dots + r_\nu(a) \text{ modulo } [p; W(a)]$$

can then be written as

$$r(a) = [\tilde{r}_1(a) \cdot e_1(a) + \tilde{r}_2(a) \cdot e_2(a) + \dots + \tilde{r}_\nu(a) \cdot e_\nu(a)] \text{ modulo } [p; W(a)] \quad (2.4.10)$$

Consider the set of all ν -tuples of the form (2.4.7) with point-wise addition and multiplication operation, the set has the structure of a commutative ring with identity. For example consider $(\tilde{r}_1(a), \dots, \tilde{r}_\nu(a))$ and $(\tilde{s}_1(a), \dots, \tilde{s}_\nu(a))$, then

$$\begin{aligned} &(\tilde{r}_1(a), \dots, \tilde{r}_\nu(a)) + (\tilde{s}_1(a), \dots, \tilde{s}_\nu(a)) \\ &= (\tilde{r}_1(a) + \tilde{s}_1(a), \dots, \tilde{r}_\nu(a) + \tilde{s}_\nu(a)) \end{aligned}$$

Additive inverse of $(\tilde{r}_1(a), \dots, \tilde{r}_\nu(a)) = (-\tilde{r}_1(a), \dots, -\tilde{r}_\nu(a))$
 $(\tilde{r}_1(a), \dots, \tilde{r}_\nu(a)) \cdot (\tilde{s}_1(a), \dots, \tilde{s}_\nu(a)) = (\tilde{r}_1(a) \cdot \tilde{s}_1(a), \dots$
 $\dots \tilde{r}_\nu(a) \cdot \tilde{s}_\nu(a))$.

With multiplicative identity $(1, \dots, 1)$. The operations $\tilde{r}_i(a) + \tilde{s}_i(a)$ and $\tilde{r}_i(a) \cdot \tilde{s}_i(a)$ are carried out modulo $[p; W_1^{h_i}(a)]$.

As seen in Section 2.1., the ring of ν -tuples is the external direct sum of ν rings. The above set of ν -tuples is the external direct sum ν local rings denoted by

$$P_p^{h_1 n_1}[W_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_\nu n_\nu}[W_\nu^{h_\nu}(a)].$$

The one-to-one correspondence between elements of $P_p^n[W(a)]$ and the ring of ν -tuples leads to the following isomorphism.

$$P_p^n[W(a)] \simeq P_p^{h_1 n_1}[W_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_\nu n_\nu}[W_\nu^{h_\nu}(a)] \quad (2.4.11)$$

and the expression on the right hand side is called the external direct sum isomorphic to $P_p^n[W(a)]$.

We note here that the components on the right hand side are primary rings. In general they are local rings; when $h_i = 1$, $P_p^{n_i}[W_i(a)]$ becomes a finite field (simple ring) of order p^{n_i} . Hence a semilocal $P_p^n[W(a)]$ is isomorphic to the external direct sum of finite number of local rings or a combination of finite fields and local rings, and a semisimple $P_p^n[W(a)]$ is isomorphic to the external sum of finite number of simple rings (in fact finite fields).

Equations(2.4.8) and (2.4.9) give the one-to-one correspondence between the internal direct sum and external direct sum components of elements in $P_p^n[W(a)]$. This leads to the isomorphism between the orthogonal ideals and the primary rings.

$$J_i \simeq P_p^{h_i n_i}[W_i^{h_i}(a)] ; \quad i = 1, 2, \dots, \nu \quad (2.4.12)$$

In general suppose R and S are two rings such that

$$R \simeq R_1 \oplus R_2 \oplus \dots \oplus R_\nu$$

and

$$S \simeq S_1 \oplus S_2 \oplus \dots \oplus S_\nu$$

and

$$S_i \simeq R_i ; \quad i = 1, 2, \dots, \nu$$

then as given in [69] $R \simeq S$.

$$\text{Thus if } P_p^n[W(a)] \simeq P_p^{h_1 n_1}[W_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_\nu n_\nu}[W_\nu^{h_\nu}(a)] \quad (2.4.13)$$

and

$$P_p^n[W'(a)] \simeq P_p^{h_1 n_1}[W_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_\nu n_\nu}[W_\nu^{h_\nu}(a)] \quad (2.4.14)$$

are such that $P_p^{h_i n_i}[W_i^{h_i}(a)] \simeq P_p^{h_i n_i}[W_i^{h_i}(a)] ; \quad i = 1, 2, \dots, \nu$

Then

$$P_p^n[W(a)] \simeq P_p^n[W'(a)] \quad (2.4.15)$$

From the internal direct sum decomposition

$$P_p^n[W(a)] = J_1 + J_2 + \dots + J_\nu ; \quad J_i \simeq P_p^{h_i n_i}[W_i^{h_i}(a)] ; \quad i = 1, 2, \dots, \nu$$

and

$$P_p^n[W'(a)] = J_1' + J_2' + \dots + J_\nu' ; \quad J_i' \simeq P_p^{h_i n_i}[W_i^{h_i}(a)] ; i = 1, 2, \dots, \nu$$

it follows that,

$$P_p^{h_i n_i}[W_i^{h_i}(a)] \simeq P_p^{h_i n_i}[W_i^{h_i}(a)] \simeq J_i \simeq J_i' ; i = 1, 2, \dots, \nu$$

(2.4.16)

The following theorem gives the condition for two residue class polynomial rings to be isomorphic.

Theorem 2.4.1

$$\text{If } W(a) = \sum_{i=1}^{\nu} W_i^{h_i}(a) \text{ and } V(a) = \sum_{i=1}^{\nu} V_i^{h_i}(a) \text{ where } W_i(a)$$

and $V_i(a)$ are irreducible polynomials of the same degree n_i (over $GF(p)$), $i = 1, 2, \dots, \nu$ then,

$$P_p^n[W(a)] \simeq P_p^n[V(a)]$$

Proof

We write the external direct sum decomposition of $P_p^n[W(a)]$ and $P_p^n[V(a)]$ and show that there is isomorphism between the direct sum components of them.

$$P_p^n[W(a)] \simeq P_p^{h_1 n_1}[W_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_\nu n_\nu}[W_\nu^{h_\nu}(a)]$$

$$P_p^n[V(a)] \simeq P_p^{h_1 n_1}[V_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_\nu n_\nu}[V_\nu^{h_\nu}(a)]$$

From Lemma 2.3.1 on the isomorphism between local rings we have,

$$P_p^{h_i n_i}[W_i^h(a)] \cong P_p^{h_i n_i}[V_i^h(a)] \quad i = 1, 2, \dots$$

Hence

$$P_p^n[W(a)] \cong P_p^n[V(a)] .$$

*

Two polynomials $W(a)$ and $V(a)$ whose irreducible factors satisfy the conditions given in Theorem 2.4.1 generate isomorphic residue class polynomial rings. This property will be made use of in Section 2.5 for enumerating nonisomorphic residue class polynomial rings.

Example 2.4.1

Consider the semisimple $P_2^3[a^3+1] = \{0, 1, a, a^2, 1+a, 1+a^2, a+a^2, 1+a+a^2\}$

$$(a^3+1) = (a+1)(a^2+a+1)$$

Let

$$W_1(a) = (a+1)$$

$$W_2(a) = (a^2+a+1)$$

Then $\overline{W_1(a)} = (a^2+a+1)$

$$\overline{W_2(a)} = (a+1)$$

There exists $b_1(a) = 1$ and $b_2(a) = a$ in $P_2^3[a^3+1]$ such that

$$\overline{W_1(a)} b_1(a) + \overline{W_2(a)} b_2(a) \equiv 1 \text{ modulo } [2; a^3+1]$$

That is, $(a^2+a+1) + (a^2+a) \equiv 1 \text{ modulo}[2; a^3+1]$.

Thus we have the orthogonal idempotents

$$e_1(a) = \overline{w_1(a)} b_1(a) = (a^2+a+1)$$

and

$$e_2(a) = \overline{w_2(a)} b_2(a) = (a^2+a)$$

It can be verified that $e_1^2(a) = e_1(a) \text{ modulo}[2; a^3+1]$

$$e_2^2(a) = e_2(a) \text{ modulo } [2; a^3+1] \text{ and } e_1(a) \cdot e_2(a) \equiv 0 \text{ modulo}[2; a^3+1] .$$

Let J_i be the ideal generated by $e_i(a)$; $i = 1, 2$,

$$\text{Then } J_1 = \langle e_1(a) \rangle = \{0, a^2+a+1\}$$

$$J_2 = \langle e_2(a) \rangle = \{0, a^2+a, 1+a^2, 1+a\}$$

and

$P_2^3[a^3+1] = J_1 + J_2 \text{ modulo}[2, a^3+1]$ is the internal direct sum decomposition of $P_2^3[a^3+1]$.

The external direct sum decomposition of $P_2^3[a^3+1]$ is,

$$P_2^3[a^3+1] \simeq P_2^1[a+1] \oplus P_2^2[a^2+a+1]$$

Further we see that

$$J_1 \simeq P_2^1[a+1] = GF(2)$$

With the correspondence $0 \neq 0$

$$(a^2+a+1) \neq 1,$$

and $J_2 \simeq P_2^2[x^2+\alpha+1] = GF(2^2)$,

with the correspondence

$$\begin{aligned} 0 &\neq 0, \\ (a^2+a) &\neq 1, \\ (a+1) &\neq \alpha, \\ (a^2+1) &\neq \alpha^2. \end{aligned}$$

In the orthogonal ideal $J_1 \simeq GF(2)$, idempotent element (a^2+a+1) plays the role of multiplicative identity. Similarly, in the orthogonal ideal $J_2 \simeq GF(2^2)$, idempotent element (a^2+a) plays the role of multiplicative identity.

In general whenever $P_p^n[W(a)]$ is semisimple the ideals generated by orthogonal idempotents are isomorphic to finite fields of the same order.

The isomorphism $\phi: P_2^3[a^3+1] \rightarrow P_2^1[a+1] \oplus P_2^2[a^2+a+1]$

gives the following correspondence between the elements in the two rings.

Let $q(a) \in P_2^3[a^3+1]$,

then $q(a) \neq [q(a) \text{ modulo } (a+1), q(a) \text{ modulo } (a^2+a+1)]$ is the corresponding element in the ring $P_2^1[a+1] \oplus P_2^2[a^2+a+1]$.

If $(\alpha(a), \beta(a)) \in P_2^1[a+1] \oplus P_2^2[a^2+a+1]$, then

$(\alpha(a), \beta(a)) \neq [\alpha(a) \cdot (a^2+a+1) + \beta(a)(a^2+a)] \text{ modulo } [2; a^3+1]$
 $\in P_2^3[a^3+1]$ is the corresponding element in $P_2^3[a^3+1]$.

*

In the external direct sum decomposition of residue class polynomial ring, the external direct sum components need not necessarily be primary rings. The component rings can as well be semilocal or semisimple rings generated by polynomials which are pairwise relatively prime. Thus, a semisimple or semilocal ring can be decomposed into smaller semisimple or semilocal rings. The internal direct sum components, which are ideals generated by orthogonal idempotents, are isomorphic to corresponding semisimple or semilocal rings.

Embedding of rings into $P_p^n[W(a)]$

As defined in Section 2.1 an injective homomorphism ϕ from a ring R to a ring S is called embedding of R into S . If R can be embedded in S , then S must contain a subring which is an isomorphic image of R . Further S itself may be isomorphic to a ring S' which contains R as a subring [69,73]. The decomposition of $P_p^n[W(a)]$ into external and internal direct sum components provides a means for obtaining the ring embedding.

Let $P_p^n[W(a)]$ be a semilocal ring where $W(a) = \prod_{i=1}^r W_i^{h_i}(a)$. Let $q_1(a)$ be a factor of $W(a)$ such that $q_1(a) \cdot q_2(a) = W(a)$ and $q_1(a)$ and $q_2(a)$ do not have any common factors. Then $P_p^n[W(a)]$ is isomorphic to $P_p^{n_1}[q_1(a)] \oplus P_p^{n_2}[q_2(a)]$, where n_i is the degree of $q_i(a)$; $i = 1, 2$, and $n_1 + n_2 = n$. Also, $P_p^n[W(a)] = J_1' + J_2'$ where J_i' is isomorphic to $P_p^{n_i}[q_i(a)]$; $i = 1, 2$. $P_p^n[W(a)]$

contains a subring (in fact an ideal) J'_1 which is isomorphic to $P_p^{n_1}[q_1(a)]$. Hence an embedding of $P_p^{n_1}[q_1(a)]$ into $P_p^n[W(a)]$ can be defined. In a specific case where $h_i = 1$ for all i and $q_1(a)$ is an irreducible factor of $W(a)$, the embedding is of finite field $P_p^{n_1}[q_1(a)]$ into semisimple $P_p^n[W(a)]$. In a more general setting a semilocal ring may be embedded into a larger semilocal ring. In all these cases the image of the embedding is an ideal in $P_p^n[W(a)]$.

The notion of embedding can be used to construct larger semisimple or semilocal $P_p^n[W(a)]$ such that there is an embedding of smaller semisimple or semilocal $P_p^{n_1}[q_1(a)]$ into $P_p^n[W(a)]$. Then $q_1(a)$ must be a factor of $W(a)$, further in the factorisation of $W(a)$ with $q_1(a)$ as a factor, the factors must be relatively prime. It is also possible to embed more than one ring say $P_p^{n_1}[q_1(a)]$, $P_p^{n_2}[q_2(a)]$.. into an appropriate larger ring $P_p^n[W(a)]$. Here the requirements are $q_1(a), q_2(a)$.. must be factors of $W(a)$ and in the factorisation of $W(a)$, the factors $q_1(a), q_2(a), \dots$, must be pairwise relatively prime. The embedding is obtained using the Chinese remainder theorem (Appendix E).

The notion of embedding of smaller rings into larger rings is used in Chapter 4 in modulation and multiplexing application of sequences over $P_p^n[W(a)]$.

Example 2.4.2

We consider embedding of $P_2^1[a+1]$ into semisimple $P_2^3[a^3+1]$.

$$(a^3+1) = (a+1)(a^2+a+1)$$

Therefore,

$$P_2^3[a^3+1] \simeq P_2^1[a+1] \oplus P_2^2[a^2+a+1]$$

and

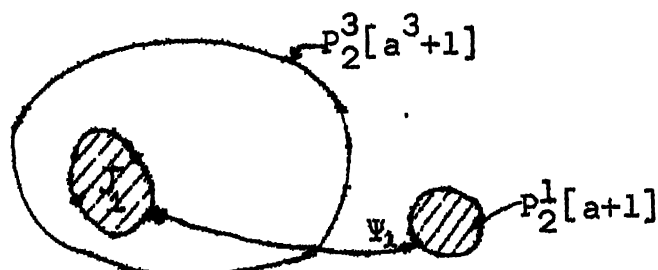
$$P_2^3[a^3+1] = \langle a^2+a+1 \rangle + \langle a^2+a \rangle \text{ modulo } [2; a^3+1].$$

We have seen in Example 2.4.1 that

$$P_2^1[a+1] \simeq \langle a^2+a+1 \rangle = J_1 = \{0, 1+a+a^2\}$$

$$P_2^2[a^2+a+1] \simeq \langle a^2+a \rangle = U_2 = \{0, a+a^2, 1+a^2, 1+a\}$$

Since $P_2^1[a+1]$ is an external direct sum component of $P_2^3[a^3+1]$, we can have embedding of $P_2^1[a+1]$ into $P_2^3[a^3+1]$. If we denote the embedding by ψ_1 , then $\psi_1: P_2^1[a+1] \rightarrow J_1$. It follows from Chinese remainder theorem,



$$\psi_1: 0 \in P_2^1[a+1] \rightarrow 0 \in J_1$$

$$\psi_1: 1 \in P_2^1[a+1] \rightarrow 1(a^2+a+1) \text{ modulo } [2; a^3+1] \in J_1$$

The inverse mapping $\Psi_1^{-1} : 0 \in J_1 \rightarrow 0 \text{ modulo } [2; a+1] \in P_2^1[a+1]$

$$\Psi_1^{-1} : (a^2+a+1) \in J_1 \rightarrow (a^2+a+1) \text{ modulo } [2; a+1] = 1 \in P_2^1[a+1].$$

Example 2.4.3

*

We consider embedding of semisimple $P_2^3[a^3+1]$ into semisimple $P_2^4[a^4+a]$.

We have, $(a^4+a) = a \cdot (a^3+1) \triangleq W_1(a) \cdot W_2(a);$

$$P_2^4[a^4+a] \simeq P_2^1[a] \oplus P_2^3[a^3+1]$$

$$\overline{W_1(a)} = (a^3+1)$$

$$\overline{W_2(a)} = a$$

There exists $b_1(a) = 1$ and $b_2(a) = a^2$ in $P_2^4[a^4+a]$ such that,

$$\overline{W_1(a)} \cdot b_1(a) + \overline{W_2(a)} \cdot b_2(a)$$

$$= (a^3+1) + a \cdot a^2 = 1 \text{ modulo } [2; a^4+a^2]$$

The orthogonal idempotents are $e_1(a) = (a^3+1)$ and $e_2(a) = a^3$, and $J_1 = \langle a^3+1 \rangle = \{0, 1+a^3\} \simeq P_2^1[a] = \{0, 1\}$

$$J_2 = \langle a^3 \rangle = \{0, a^3, a, a^2, a+a^3, a^2+a^3, a+a^2, a+a^2+a^3\}$$

$$\simeq P_2^3[a^3+1] = \{0, 1, a, a^2, (1+a), (1+a^2), (a+a^2) \\ 1+a+a^2\}$$

Let $\Psi: P_2^3[a^3+1] \rightarrow J_2$ be the embedding.

Then $\forall r(a) \in P_2^3[a^3+1]$, $\Psi(r(a)) = r(a)a^3 \text{ modulo } [2; a^4+a] \in J_2$

and $\Psi^{-1}: J_2 \rightarrow P_2^3[a^3+1]$

$\forall j(a) \in J_2 \quad \Psi^{-1}(j(a)) = j(a) \text{ modulo } [2; a^3+1] \in P_2^3[a^3+1].$

*

Decomposition of Modules

The results obtained on decomposition of rings may be used to decompose modules defined over these rings.

Let $W(a) = \prod_{i=1}^{\nu} W_i^{h_i}(a)$; $W_i(a)$ irreducible polynomial over $GF(p)$. Consider the ring $P_p^n[W(a)]$. The set of all K -tuples over $P_p^n[W(a)]$ constitutes a $P_p^n[W(a)]$ -module S of rank K .

We have $P_p^n[W(a)] = J_1 + J_2 + \dots + J_\nu$

where J_i is the ideal generated by orthogonal idempotent $e_i(a)$

and $J_i \simeq P_p^{h_i n_i} [W_i^{h_i}(a)]$. Any element $r(a) \in P_p^n[W(a)]$ can be uniquely expressed as

$$r(a) = r_1(a) + r_2(a) + \dots + r_\nu(a); \quad r_i(a) \in J_i.$$

Consider the set of all K -tuples over J_i .

This constitutes a $P_p^n[W(a)]$ -submodule S_i of module S ;

$i = 1, 2, \dots, \nu$

From the properties of J_i it follows that

$$S_i \cap (S_1 + S_2 + \dots + S_{i-1} + S_{i+1} + \dots + S_\nu) = 0$$

and hence the submodules are said to be independent. Any element $s \in S$ can be uniquely expressed as

$$s = s_1 + s_2 + \dots + s_\nu ; \quad s_i \in S_i \quad i = 1, 2, \dots, \nu$$

and

$$S = S_1 + S_2 + \dots + S_\nu \quad (2.4.17)$$

$P_p^n[W(a)]$ -module S is said to be the internal direct sum of the submodules S_1, S_2, \dots, S_ν .

We also have

$$P_p^n[W(a)] \simeq P_p^{n_1}[W_1^{h_1}(a)] \oplus P_p^{n_2}[W_2^{h_2}(a)] \oplus \dots \oplus P_p^{n_\nu}[W_\nu^{h_\nu}(a)]$$

$$J_i \simeq P_p^{h_i n_i}[W_i^{h_i}(a)] ; \quad i = 1, 2, \dots, \nu$$

Any element $r(a) \in P_p^n[W(a)]$ has a one-to-one correspondence with the ν -tuple

$$r(a) \rightleftharpoons (\tilde{r}_1(a), \tilde{r}_2(a), \dots, \tilde{r}_\nu(a))$$

where $\tilde{r}_i(a) \in P_p^{h_i n_i}[W_i^{h_i}(a)] ; \quad i = 1, 2, \dots, \nu$

This implies that, $S \simeq \tilde{S}_1 \oplus \tilde{S}_2 \oplus \dots \oplus \tilde{S}_\nu$ (2.4.18)

where \tilde{S}_i is the set of all K -tuples from $P_p^{h_i n_i}[W_i^{h_i}(a)]$
 $i = 1, 2, \dots, \nu$.

(2.4.18) is called the external direct sum of the module S .

Example 2.4.4

Consider the ring $P_2^3[a^3+1]$.

$$P_2^3[a^3+1] = \langle a^2+a+1 \rangle + \langle a^2+a \rangle$$

$$P_2^3[a^3+1] \simeq P_2^1[a+1] \oplus P_2^2[a^2+a+1]$$

$$P_2^3[a^3+1] = \{0, 1, a, a^2, (1+a), (1+a^2), (a+a^2), (1+a+a^2)\}$$

Consider the set of all 2-tuples over $P_2^3[a^3+1]$. This constitutes a $P_2^3[a^3+1]$ -module S of rank 2.

$$\langle a^2+a+1 \rangle = \{0, a^2+a+1\}$$

$$\langle a^2+a \rangle = \{0, (1+a), (a+a^2), (1+a^2)\}$$

The set of all 2-tuples over $\langle a^2+a+1 \rangle$ constitutes the submodule S_1 and the set of all 2-tuples over $\langle a^2+a \rangle$ constitutes the submodule S_2 .

$$S = S_1 + S_2$$

Let $s = ((1+a^2), (1+a+a^2)) \in S$.

then $s_1 = (0, 1+a+a^2) \in S_1$

$$s_2 = (1+a^2, 0) \in S_2$$

$$s = s_1 + s_2$$

$$\langle a^2+a+1 \rangle \simeq P_2^1[a+1] \text{ and } \langle a^2+a \rangle \simeq P_2^2[a^2+a+1]$$

The set of all two tuples over $P_2^1[a+1]$ constitutes

$$P_2^1[a+1]\text{-module } \tilde{S}_1 \simeq S_1.$$

The set of all two tuples over $P_2^2[a^2+a+1]$ constitutes

$$P_2^2[a^2+a+1]\text{-module } \tilde{S}_2 \simeq S_2$$

Let $s = ((1+a), (1+a+a^2)) \in S$

$$s \simeq (\tilde{s}_1, \tilde{s}_2) = \tilde{s}$$

$$\text{then } \tilde{s}_1 = [(0 \ 1), (a, 0)]$$

$$\text{where } (1+a^2) \simeq (0, a)$$

$$(a^2+a+1) \simeq (1, 0).$$

*

2.4.2 Decomposition of $\bigotimes_{(x)}^T \{P_p^{n_i}[W_i(a_i)]\}$

Results of the residue class polynomial ring $P_p^n[W(a)]$ can be extended to decomposition of tensor product of residue class polynomial rings.

$$\text{Suppose } P_p^{n_w}[W(a)] \simeq P_p^{h_1 n_{w1}}[W_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_{\nu} n_{w\nu}}[W_{\nu}^{h_{\nu}}(a)]$$

Then,

$$P_p^{n_v}[V(b)] \otimes P_p^{n_w}[W(a)] \text{ is isomorphic to}$$

$$(P_p^{n_v}[V(b)] \otimes P_p^{h_1 n_{w1}}[W_1^{h_1}(a)] \oplus (P_p^{n_v}[V(b)] \otimes P_p^{h_2 n_{w2}}[W_2^{h_2}(a)])) \\ \oplus \dots \oplus (P_p^{n_v}[V(b)] \otimes P_p^{h_{\nu} n_{w\nu}}[W_{\nu}^{h_{\nu}}(a)]).$$

$$\text{If } P_p^{n_v}[V(b)] \simeq P_p^{\eta_1 n_{v1}}[V_1^{\eta_1}(b)] \oplus \dots \oplus P_p^{\eta_s n_{vs}}[V_s^{\eta_s}(b)] \text{ then,}$$

$$P_p^{n_v}[V(b)] \otimes P_p^{n_w}[W(a)] \quad (2.4.19)$$

is isomorphic to the direct sum of all tensor products

$$p_p^{\eta_i n_{vi}}[V_i^{\eta_i}(b)] \otimes p_p^{h_j n_{wj}}[W_j^{h_j}(a)] \quad \begin{array}{l} i = 1, 2, \dots, s \\ j = 1, 2, \dots, \nu \end{array} \quad (2.4.20)$$

Corresponding to each element of the tensor product residue class polynomial ring given in Equation (2.4.19) we have $s\nu$ -tuple.

Example 2.4.5

Consider the tensor product of a semilocal $P_2^6[a^6+1]$ and semisimple $P_2^3[b^3+1]$.

$$\text{That is, } P_2^6[a^6+1] \overset{T}{\otimes} P_2^3[b^3+1] \quad (2.4.21)$$

$$\text{we have, } P_2^6[a^6+1] \simeq P_2^4[(a^2+a+1)^2] \oplus P_2^2[(a+1)^2]$$

$$\text{and } P_2^3[b^3+1] \simeq P_2^2[(b^2+b+1)] \oplus P_2^1[(b+1)] .$$

Hence,

$$\begin{aligned} P_2^6[a^6+1] \overset{T}{\otimes} P_2^3[b^3+1] &\simeq (P_2^4[(a^2+a+1)^2] \overset{T}{\otimes} P_2^2[(b^2+b+1)]) \\ &\oplus (P_2^4[(a^2+a+1)^2] \overset{T}{\otimes} P_2^1[(b+1)]) \\ &\oplus (P_2^2[(a+1)^2] \overset{T}{\otimes} P_2^2[(b^2+b+1)]) \oplus (P_2^2[(a+1)^2] \overset{T}{\otimes} \\ &P_2^1[(b+1)]) . \end{aligned} \quad (2.4.22)$$

The elements of the tensor product ring given by (2.4.21) are the linear combinations over $GF(2)$ of the elements

$$\{1, a, a^2, a^3, a^4, a^5$$

$$b, ab, a^2b, a^3b, a^4b, a^5b$$

$b^2, ab^2, a^2b^2, a^3b^2, a^4b^2, a^5b^2\}$ and hence there are 2^{18} elements in this ring.

For each element of the tensor product ring, there is a 4-tuple in the external direct sum given by the expression (2.4.22). For example, $1+a^5b^2$ is an element in the ring given by (2.4.21). The corresponding 4-tuple, which is the external direct sum of $1+a^5b^2$ is written as ,

$$\begin{aligned} & \{(1 \bmod [2; (a^2+a+1)^2] \cdot 1 \bmod [2; (b^2+b+1)] + (a^5 \bmod [2; \\ & (a^2+a+1)^2] \cdot b^2 \bmod [2; (b^2+b+1)]), \\ & ((1 \bmod [2; (a^2+a+1)^2] \cdot 1 \bmod [2; (b+1)] + (a^5 \bmod [2; \\ & (a^2+a+1)^2] \cdot b^2 \bmod [2; b+1)]), \\ & (1 \bmod [2; (a+1)^2] \cdot 1 \bmod [2; (b^2+b+1)] + (a^5 \bmod [2; \\ & (a+1)^2] \cdot b^2 \bmod [2; (b^2+b+1)]), \\ & (1 \bmod [2; (a+1)^2] \cdot 1 \bmod [2; b+1] + (a^5 \bmod [2; \\ & (a+1)^2] \cdot b^2 \bmod [2; (b+1)])\}; \end{aligned}$$

$$= \{1+(a^3+a)(b+1), 1+(a^3+a).1, 1+(a).(b+1), 1+a.1\}$$

$$= \{(1+a+a^3+ab+a^3b), (1+a+a^3), (1+a+ab), (1+a)\} .$$

2.5 ENUMERATION OF NONISOMORPHIC RESIDUE CLASS RINGS OF POLYNOMIALS OVER $GF(p)$

It is known that finite fields of the same order are all isomorphic to each other [18,60,62,69]. However, in a ring this is not true. It will be seen that for $n > 1$ there are more than one residue class polynomial rings, which are not isomorphic to each other. The set of isomorphic residue class polynomial rings of a given order p^n constitutes an equivalence class. The number of such classes is equal to the number of nonisomorphic residue class polynomial rings of order p^n .

Consider the monic polynomials of degree n over $GF(p)$. Their number is p^n . Each of the p^n polynomials generates a residue class ring, some of which are isomorphic to each other. Any polynomial of degree n can be expressed as a unique product of powers of irreducible polynomials. The isomorphism and decomposition theorem of Sections 2.3 and 2.4 are used to classify the p^n residue class polynomial rings depending on the factors of the polynomials of degree n . Towards this end consider the following example.

Example 2.5.1

Let $p = 2$ and $n = 2$. The number of polynomials of degree 2 over $GF(2)$ is 4. They are

- i) (a^2+a+1) : Irreducible polynomial of degree 2 over $GF(2)$
- ii) $a^2, (a+1)^2$: Square of irreducible polynomial of degree 1
- iii) $a(a+1)$: Product of two irreducible polynomials of degree 1.

From Lemma 2.3.1 we have $P_2^2[a^2] \simeq P_2^2[a^2+1]$. The above four rings are classified into different classes such that each class contains isomorphic rings

$$\{P_2^2[a^2+a+1]\}, \{P_2^2[a^2], P_2^2[a^2+1]\} \text{ and } \{P_2^2[a(a+1)]\}$$

Thus the number of nonisomorphic residue class polynomial rings of order 2^2 over $GF(2)$ is 3.

From the point of convenience the polynomials can be written in terms of degrees of irreducible polynomials. For example, (2) specifies irreducible polynomials of degree 2 over $GF(2)$. (a^2+a+1) is the only irreducible polynomial of degree 2 over $GF(2)$, and (11) specifies products of irreducible polynomials of degree 1 or square of an irreducible polynomial of degree 1. Such polynomials are $a^2, (a+1)^2, a(a+1)$.

It is seen that (2) and (11) are two ways of representing the integer 2 as sum of positive integers, called the partitions of integer 2.

In general, let β be a positive integer. Consider the representations of β as a sum of positive integers $\beta_0, \beta_1, \dots, \beta_{s-1}$, i.e.,

$$\beta = \beta_0 + \beta_1 + \dots + \beta_{s-1} \quad (2.5.1)$$

where s is a positive integer at most equal to β . Representations of the form (2.5.1) are called partitions of an integer β into positive integer summands $\beta_0, \beta_1, \dots, \beta_{s-1}$. Thus the integer β has the following partitions

(11111), (221), (2111), (32), (311), (41), (5)

The number of partitions of an integer β is known as partition function and is denoted by $\alpha(\beta)$. Two partitions are not considered to be different if they differ only in the order of their summands. $\alpha(0)$ is taken to be 1.

Example 2.5.2

1) $\alpha(1) = 1, \alpha(2) = 2, \alpha(5) = 7.$

Table 2.5.1 gives the partitions of integers from 1 to 7.

Additional examples are taken up now to show how the number of classes of residue class polynomial rings are related to partition function.

Table 2.5.1 Partitions of integers from 1 to 7

n	$\alpha(n)$	Partitions
1	1	(1)
2	2	(11), (2)
3	3	(111), (12), (3)
4	5	(1111), (211), (22), (31), (4)
5	7	(11111), (2111), (221), (311), (32), (41), (5)
6	11	(111111), (21111), (2211), (222), (3111), (321), (33), (411), (42), (51), (6)
7	15	(1111111), (211111), (22111), (2221), (31111), (3211), (322), (331), (4111), (421), (43), (511), (52), (61), (7)

Example 2.5.3

Let $p = 2$; $n = 3$. The number of polynomials of degree 3 over $\text{GF}(2)$ is $2^3 = 8$. They are listed below using partitions of 3.

- (i) (3) specifies irreducible polynomials of degree 3. They are, (a^3+a+1) , (a^3+a^2+1) .

- ii) (21) specifies products of irreducible polynomials of degree 2 and degree 1. They are, $(a^2+a+1)a$; $(a^2+a+1)(a+1)$.
- iii) (111) specifies products of irreducible polynomials of degree 1 or their power. They are, a^3 , $(a+1)^3$, $a^2(a+1)$, $a(a+1)^2$.

From Lemma 2.3.1,

$$P_2^3[a^3+a+1] \simeq P_2^3[a^3+a^2+1]$$

$$P_2^3[a^3] \simeq P_2^3[(a+1)^3]$$

From Theorem 2.4.1,

$$P_2^3[(a^2+a+1)a] \simeq P_2^3[(a^2+a+1)(a+1)] \quad \text{and}$$

$$P_2^3[a^2(a+1)] \simeq P_2^3[(a+1)^2a]$$

The above rings are classified such that each class contains isomorphic rings.

$$\{P_2^3[a^3+a+1], \quad P_2^3[a^3+a^2+1]\}$$

$$\{P_2^3[(a^2+a+1)a], P_2^3[(a^2+a+1)(a+1)]\}$$

$$\{P_2^3[a^3], \quad P_2^3[(a+1)^3]\}$$

$$\{P_2^3[a^2(a+1)], \quad P_2^3[(a+1)^2a]\}$$

Thus the number of nonisomorphic residue class rings of polynomials over GF(2), generated by polynomials of degree 3 is 4.

*

Example 2.5.4

$p = 2, n = 4$. The number of polynomials of degree 4 over $GF(2)$ is $2^4 = 16$. They are listed below using partitions of 4.

- i) (4) specifies irreducible polynomials of degree 4. They are : $(a^4+a+1), (a^4+a^3+1), (a^4+a^3+a^2+a+1)$
- ii) (31) specifies products of irreducible polynomials of degree 3 and degree 1. They are : $(a^3+a+1)a, (a^3+a+1)(a+1), (a^3+a^2+1)a, (a^3+a^2+1)(a+1)$.
- iii) (211) specifies products of irreducible polynomials of degree 2 and 1. They are : $(a^2+a+1)a^2, (a^2+a+1)(a+1)^2, (a^2+a+1)(a+1)(a)$.
- iv) (22) specifies products of irreducible polynomials of degree 2, that is, $(a^2+a+1)(a^2+a+1)$.
- vi) (1111) specifies products of irreducible polynomials of degree 1, they are : $a^4, (a+1)^4, a^3(a+1), (a+1)^3a, a^2(a+1)^2$

Using the Lemma 2.3.1 and Theorem 2.4.1, the 16 rings are classified into classes such that rings which are isomorphic to each other are in the same class. The classes are :

$$\{P_2^4[a^4+a+1], P_2^4[a^4+a^3+1], P_2^4[a^4+a^3+a^2+a+1]\}$$

$$\{P_2^4[(a^3+a+1)a], P_2^4[(a^3+a+1)(a+1)], P_2^4[(a^3+a^2+1)a],$$

$$P_2^4[(a^3+a^2+1)(a+1)]\}$$

Example 2.5.4

$p = 2$, $n = 4$. The number of polynomials of degree 4 over $GF(2)$ is $2^4 = 16$. They are listed below using partitions of 4.

- i) (4) specifies irreducible polynomials of degree 4. They are : (a^4+a+1) , (a^4+a^3+1) , $(a^4+a^3+a^2+a+1)$
- ii) (31) specifies products of irreducible polynomials of degree 3 and degree 1. They are : $(a^3+a+1)a$, $(a^3+a+1)(a+1)$, $(a^3+a^2+1)a$, $(a^3+a^2+1)(a+1)$.
- iii) (211) specifies products of irreducible polynomials of degree 2 and 1. They are : $(a^2+a+1)a^2$, $(a^2+a+1)(a+1)^2$, $(a^2+a+1)(a+1)(a)$.
- iv) (22) specifies products of irreducible polynomials of degree 2, that is, $(a^2+a+1)(a^2+a+1)$.
- vi) (1111) specifies products of irreducible polynomials of degree 1, they are : a^4 , $(a+1)^4$, $a^3(a+1)$, $(a+1)^3a$, $a^2(a+1)^2$

Using the Lemma 2.3.1 and Theorem 2.4.1, the 16 rings are classified into classes such that rings which are isomorphic to each other are in the same class. The classes are :

$$\{P_2^4[a^4+a+1], P_2^4[a^4+a^3+1], P_2^4[a^4+a^3+a^2+a+1]\}$$

$$\{P_2^4[(a^3+a+1)a], P_2^4[(a^3+a+1)(a+1)], P_2^4[(a^3+a^2+1)a],$$

$$P_2^4[(a^3+a^2+1)(a+1)]\}$$

$$\{P_2^4[(a^2+a+1)a^2], P_2^4[(a^2+a+1)(a+1)^2]\}$$

$$\{P_2^4[(a^2+a+1)(a+1)a]\}, \{P_2^4[(a^2+a+1)^2]\}$$

$$\{P_2^4[a^4], P_2^4[a^4+1]\}, \{P_2^4[(a+1)a^3], P_2^4[a(a+1)^3]\}$$

$$\{P_2^4[a^2(a+1)^2]\}.$$

There are in all 8 classes and therefore, the number of non-isomorphic residue class polynomial rings generated by polynomials over GF(2) of degree 4 in one variable is 8. *

In the above examples the partitions of $n = 2, 3$ and 4 are used for listing the polynomials of degree $n = 2, 3$ and 4 respectively. We have classified the polynomials of a given degree into classes such that polynomials belonging to the same class generate isomorphic residue class polynomial rings. Corresponding to each partition of n , the polynomials are listed in terms of factors of irreducible polynomials or its powers. If a partition of n contains only distinct integers, then the corresponding polynomials are products of irreducible polynomials. If a partition of n contains integers which repeat, then the polynomials are powers of irreducible polynomials or products of irreducible polynomials of the same degree. The restricted partition function helps in getting the number of distinct (nonisomorphic) classes of residue class polynomial

rings over $GF(p)$ corresponding to a partition n , without listing the polynomials. Corresponding to each partition of n the number of nonisomorphic residue class polynomial rings are determined which are finally added to get the total number of residue class polynomial rings of order p^n . Towards this end we first explain the term restricted partition function, then we consider typical partitions of n and obtain expression for the number of nonisomorphic residue class polynomial rings, corresponding to these partitions.

The number of partitions of β into summands less than or equal to η denoted by $\alpha_\eta(\beta)$ is called the restricted partition function [55].

Example 2.5.5

- i) The number of partitions of 5 into summands less than or equal to 2, is three. They are (5), (41), (32). Hence $\alpha_2(5) = 3$.
- ii) The number of partitions of 6 into summands less than or equal to 3, is seven. They are : (6), (51), (42), (411), (33), (321), (222). Hence, $\alpha_3(6) = 7$. *

Functions $\alpha(\beta)$ and $\alpha_\eta(\beta)$ have the following properties [55] :

- i) $\alpha_\eta(\beta) = \alpha(\beta)$ if $\beta \leq \eta$
- ii) $\alpha_\eta(\beta) \leq \alpha(\beta)$ $\forall \beta \geq 0$
- iii) $\alpha_\eta(\beta) = \alpha_{\eta-1}(\beta) + \alpha_\eta(\beta-\eta)$ if $\beta \geq \eta > 1$ (2.5.2)

The recurrence relation given by (2.5.2) can be used to find $\alpha_\eta(\beta)$ in terms of $\alpha_j(i)$, $i < \beta$ and $j \leq \eta$ or $i \leq \beta$ and $j < \eta$. These concepts are used in the determination of nonisomorphic residue class rings of polynomials over $GF(p)$.

We now obtain expression for the number of nonisomorphic residue class polynomial rings of order p^n , corresponding to typical partition of n .

Let one of the partitions of n be

$$(j, j, \dots, j) \quad (2.5.3)$$

where j repeats e_j times. Let the number of irreducible polynomials of degree j over $GF(p)$ be η_j . (The determination of the number η_j of irreducible polynomials of degree j over a finite field q is discussed in Appendix A).

Lemma 2.5.1

The number of nonisomorphic residue class rings of polynomials over $GF(p)$ generated by polynomials corresponding to the partition of n of the form given in (2.5.3) is $\alpha_{\eta_j}(e_j)$; the partitions of e_j restricted to number of summands less than or equal to η_j .

- i) $\alpha_\eta(\beta) = \alpha(\beta)$ if $\beta \leq \eta$
- ii) $\alpha_\eta(\beta) \leq \alpha(\beta)$ $\forall \beta \geq 0$
- iii) $\alpha_\eta(\beta) = \alpha_{\eta-1}(\beta) + \alpha_\eta(\beta-\eta)$ if $\beta \geq \eta > 1$ (2.5.2)

The recurrence relation given by (2.5.2) can be used to find $\alpha_\eta(\beta)$ in terms of $\alpha_j(i)$, $i < \beta$ and $j \leq \eta$ or $i \leq \beta$ and $j < \eta$. These concepts are used in the determination of nonisomorphic residue class rings of polynomials over $GF(p)$.

We now obtain expression for the number of nonisomorphic residue class polynomial rings of order p^n , corresponding to typical partition of n .

Let one of the partitions of n be

$$(j, j, \dots, j) \quad (2.5.3)$$

where j repeats e_j times. Let the number of irreducible polynomials of degree j over $GF(p)$ be η_j . (The determination of the number η_j of irreducible polynomials of degree j over a finite field q is discussed in Appendix A).

Lemma 2.5.1

The number of nonisomorphic residue class rings of polynomials over $GF(p)$ generated by polynomials corresponding to the partition of n of the form given in (2.5.3) is $\alpha_{\eta_j}(e_j)$; the partitions of e_j restricted to number of summands less than or equal to η_j .

Proof :

Let the η_j irreducible polynomials of degree j over $GF(p)$ be $W_1(a), W_2(a), \dots, W_{\eta_j}(a)$. A polynomial of degree n which is the product of these polynomials is of the form

$$W_1^{k_1}(a) W_2^{k_2}(a) \dots W_{\eta_j}^{k_{\eta_j}}(a)$$

where

$$\sum_{i=1}^{K_{\eta_j}} k_i = e_j$$

Suppose we indicate the values taken by $k_1, k_2, \dots, k_{\eta_j}$ as a η_j -tuple $(c_1, c_2, \dots, c_{\eta_j})$ such that $\sum_{i=1}^{\eta_j} c_i = e_j$. We see that a given set of values of $(k_1, k_2, \dots, k_{\eta_j})$, that is, $(c_1, c_2, \dots, c_{\eta_j})$ corresponds to a residue class polynomial ring generated by $P_p^n[\prod_{i=1}^{\eta_j} W_i^{c_i}(a)]$. Since each $W_i(a); i = 1, 2, \dots, \eta_j$ is a distinct irreducible polynomial of the same degree j , if the arrangement of $(c_1, c_2, \dots, c_{\eta_j})$ is changed to any other form, from Lemma 2.3.1, we see that the resulting residue class polynomial rings are isomorphic to each other. In other words the residue class polynomial rings generated by all polynomial products $W_1^{c_1}(a), W_2^{c_2}(a), \dots, W_{\eta_j}^{c_{\eta_j}}(a)$, resulting from reordering their powers $(c_1, c_2, \dots, c_{\eta_j})$ are isomorphic. Therefore, for computing nonisomorphic residue class polynomial rings, it is enough if we consider the partitions of e_j restricted to summands less than or equal to η_j . The number of residue class

polynomial rings corresponding to the partitions of $n = (j, \dots, j)$; j occurring e_j times is therefore equal to $\alpha_{\eta_j}(e_j)$. *

Next we consider a partition of the type

$$(r_1, \dots, r_1, r_2, \dots, r_2, \dots, r_j, \dots, r_j) \quad (2.5.4)$$

where r_i repeats e_i times, $i = 1, 2, \dots, j$. Let the number of irreducible polynomials of degree r_i over $GF(p)$ be η_{r_i} .

Lemma 2.5.2

The number of nonisomorphic residue class polynomial rings over $GF(p)$ generated by polynomials corresponding to the partition of n of the form (2.5.4) is given by

$$\prod_{i=1}^j \alpha_{\eta_{r_i}}(e_i) \quad (2.5.5)$$

Proof

From the result of Lemma 2.5.1, the number of nonisomorphic residue class polynomial rings corresponding to the partition n of the form (2.5.4) with the irreducible polynomials of degree r_1, r_2, \dots, r_{j-1} fixed, is given by $\alpha_{n_{r_j}}(e_j)$. Likewise the number of nonisomorphic residue class r_j polynomial rings, with all irreducible polynomials of degree $r_1, r_2, \dots, r_{i-1}, r_{i+1}, \dots, r_j$, fixed except r_i , is given by $\alpha_{n_{r_i}}(e_i)$. Hence the number of nonisomorphic residue class polynomial rings corresponding to the partition of n given by (2.5.4) is $\prod_{i=1}^j \alpha_{\eta_{r_i}}(e_i)$. *

Theorem 2.5.1

Let n be any positive integer. The number of nonisomorphic residue class polynomial rings of order p^n over $GF(p)$, generated by polynomials in one variable is given by

$$\sum_{\text{partitions of } n} \prod_{i=1}^n \alpha_{\eta_i}(e_i) \quad (2.5.6)$$

where the summation is over all the partitions of n , e_i is the number of repetitions of the integer i in the particular partition and η_i is the number of i th degree irreducible polynomials over $GF(p)$. We define $\alpha_{\eta_i}(0) = 1, \forall \eta_i$.

Proof

Follows from Lemmas 2.5.1 and 2.5.2.

*

Example 2.5.6

Number of nonisomorphic residue class polynomial rings generated by polynomials of degree 4 over $GF(3)$. We have $p = 3, n = 4$.

The number of irreducible polynomials η_i of degree i over $GF(3)$ $i = 1, 2, 3, 4$ is obtained from Table 2.5.2 or can be computed as indicated in Appendix A. We have $\eta_1 = 3, \eta_2 = 3, \eta_3 = 8, \eta_4 = 18$. Applying Theorem 2.5.1 the number of nonisomorphic residue class polynomial rings, generated by polynomials of degree 4 over $GF(3)$ is

$$\begin{aligned}
& \sum_{\substack{[4],[31],[211], \\ [22],[1111]}} \prod_{i=1}^n \alpha_{\eta_i}(e_i) \\
&= \alpha_{\eta_4}(e_4) + [\alpha_{\eta_3}(e_3) \cdot \alpha_{\eta_1}(e_1)] + [\alpha_{\eta_2}(e_2) \cdot \alpha_{\eta_1}(e_1)] + \alpha_{\eta_2}(e_2) + \alpha_{\eta_1}(e_1) \\
&= \alpha_{18}(1) + [\alpha_3(1) \cdot \alpha_3(1)] + [\alpha_3(1) \cdot \alpha_3(2)] + \alpha_3(2) + \alpha_3(4) \\
&= 1 + 1 \cdot 1 + 1 \cdot 2 + 2 + 4 \\
&= 10 .
\end{aligned}$$

*

The number of irreducible polynomials of degree n over $GF(p)$, the number of nonisomorphic residue class rings of polynomials over $GF(p)$ of order p^n , which we have called distinct classes, for $p = 2, 3, 5$ and $n = 1, 2, 3, 4, 5, 6, 7$ and the partition function of n are given in Tables 2.5.2 and 2.5.3 respectively.

We have seen that the number of nonisomorphic residue class polynomial rings $P_p^n[W(a)]$ is a function of the number of irreducible polynomials over $GF(p)$ of degree $\leq n$ and the restricted partition function of integers $\leq n$, where n is the degree of $W(a)$. If n is a prime number there is no other nonisomorphic residue class ring of polynomials of order p^n , in one variable. However, if n is a composite number there are residue class rings of polynomials in more than one variable. These can be shown to be an appropriate tensor products of residue class polynomial rings. The isomorphism in tensor product residue

Table 2.5.2 Number of irreducible polynomials of degree i over $GF(p)$

η_i : Number of irreducible polynomials of degree i			
i	$p = 2$	$p = 3$	$p = 5$
1	2	3	5
2	1	3	10
3	2	8	40
4	3	18	150
5	6	48	624
6	9	116	2305
7	18	312	11160

Table 2.5.3 Number of distinct classes of residue class ring of polynomials over $GF(p)$
 $P_p^n[W(a)]$ of order p^n

Number of distinct classes of residue class ring of polynomials of order p^n , over $GF(p)$			
n	$p = 2$	$p = 3$	$p = 5$
1	1	1	1
2	3	3	3
3	4	5	5
4	8	10	11
5	11	15	17
6	20	29	33
7	27	42	50

class polynomial rings is discussed in Section 2.2. As seen in Subsection 2.2.3 the tensor product of two residue class polynomial rings may be isomorphic to a residue class polynomial ring in one variable. In general, tensor product of j residue class polynomial rings may be isomorphic to tensor product of $(j-1)$ or less residue class polynomial rings. This topic needs further investigation. However, we do not go into the details.

2.6 RINGS ISOMORPHIC TO RESIDUE CLASS RINGS OF POLYNOMIALS OVER $GF(p)$

In the case of finite fields, $GF(p^n)$ it is known that there exists a one-to-one correspondence between the field elements and n -tuples over $GF(p)$, which enables one to obtain LSS over $GF(p)$ isomorphic to LSS over $GF(p^n)$ [8,12,13,18,21]. This one-to-one correspondence can be extended to $P_p^n[W(a)]$ or $\bigotimes^T P_p^{n_i}[W_i(a_i)]$ leading to LSS over $GF(p)$ which are isomorphic to LSS over $P_p^n[W(a)]$ or $\bigotimes^T P_p^{n_i}[W_i(a_i)]$, the details of which are given in Section 3.4. Here we show that for each residue class ring of polynomials over $GF(p)$, there exists isomorphic rings of $n \times n$ matrices and n -tuples over $GF(p)$. Addition and multiplication operations in the case of ring of $n \times n$ matrices over $GF(p)$ are the usual matrix addition and multiplication respectively, modulo p . Addition operation in the case of ring of n -tuples over $GF(p)$ is pointwise addition

modulo p , while the multiplication of any two n -tuples in this ring becomes an appropriate matrix vector multiplication over $GF(p)$. Rings isomorphic to $P_p^n[W(a)]$ are called family of rings.

First we obtain rings of $n \times n$ matrices isomorphic to given $P_p^n[W(a)]$.

2.6.1 Ring $M_p^n[W]$ of $n \times n$ Matrices over $GF(p)$ Isomorphic to $P_p^n[W(a)]$

Let $W(a) = a^n + w_{n-1}a^{n-1} + \dots + w_1a + w_0$; with coefficients $w_i \in GF(p)$. The $n \times n$ matrix

$$W = \begin{bmatrix} 0 & 0 & \dots & 0 & -w_0 \\ 1 & 0 & \dots & 0 & -w_1 \\ & 1 & \dots & 0 & \vdots \\ & & \ddots & 1 & -w_{n-2} \\ & & & 1 & -w_{n-1} \end{bmatrix}$$

associated with $W(a)$ is called its companion matrix [12,13,14, 57]. It may be noted that the elements of W are from $GF(p)$. The polynomial $W(a)$ is the characteristic polynomial of W and by Cayley-Hamilton theorem,

$$W^n + w_{n-1}W^{n-1} + \dots + w_1W + w_0 I = \underline{0} \quad (2.6.1)$$

where $\underline{0}$ is $n \times n$ null matrix

$W(a)$ is also the minimal polynomial of W . For obtaining a ring of $n \times n$ matrices over $GF(p) \cong P_p^n[W(a)]$ the following Lemmas are proved first.

Lemma 2.6.1

The $n \times n$ matrices in the set

$$\{I, W, W^2, \dots, W^{n-1}\} \quad (2.6.2)$$

are linearly independent over $GF(p)$.

Proof

Since $W(a)$ is the minimal polynomial of W any nonzero polynomial in W of degree $(n-1)$ or less over $GF(p)$ is not a null matrix. That is,

$$\sum_{i=0}^{n-1} q_i W^i = \underline{0}, \quad q_i \in GF(p) \text{ implies } q_i = 0 \text{ for all } i.$$

Hence the matrices in the set given by (2.6.2) are linearly independent over $GF(p)$. *

Lemma 2.6.2

Linear combinations of matrices from the set (2.6.2) are unique.

Proof

Consider the following two linear combinations $\sum_{i=0}^{n-1} q_i W^i \triangleq Q$

and $\sum_{i=0}^{n-1} g_i W^i \triangleq G$; $q_i, g_i \in GF(p)$ and $q_i \neq g_i$ for at least one value of i from the set $\{0, 1, \dots, n-1\}$. Suppose $Q=G$, then

$$\sum_{i=0}^{n-1} (q_i - g_i) W^i = \underline{0}.$$

From the result of the Lemma 2.6.1 this implies $(q_i - g_i) = 0$ that is $q_i = g_i$ for all $i = 0, 1, \dots, n-1$. This is a contradiction. Hence, Q is not equal to G .

*

Theorem 2.6.1

The set of all linear combinations of matrices over $GF(p)$ from the set $\{I, W, \dots, W^{n-1}\}$, with usual matrix addition and multiplication modulo p , constitutes a commutative ring $M_p^n[W]$ of order p^n .

Proof

From Lemma 2.6.2, we see that distinct linear combination of matrices from the set are distinct. Any typical element of $M_p^n[W]$ is of the form $\sum_{i=0}^{n-1} q_i W^i$; $q_i \in GF(p)$; $i = 0, \dots, n-1$. Therefore, the order of $M_p^n[W]$ is p^n .

$M_p^n[W]$ satisfies the axioms of a commutative ring.

1. It is an abelian group under usual matrix addition modulo p .
2. Multiplication is matrix multiplication modulo p . Multiplication of any two elements in $M_p^n[W]$ gives a polynomial in W whose degree is $\leq 2n-2$. Since W satisfies $W(a)$ we have

$$W^n = - \sum_{i=0}^{n-1} w_i W^i$$

Thus any power of W say W^j for $j \geq n$ is a polynomial in W whose degree is less than or equal to $n-1$, and multiplication operation in $M_p^n[W]$ is closed.

3. Multiplication is associative.
4. The operations satisfy distributive laws.
5. Powers of W commute under multiplication therefore in $M_p^n[W]$ multiplication is commutative.

Hence $M_p^n[W]$ is a commutative ring. of $n \times n$ matrices of order p^n .

*

Theorem 2.6.2

$M_p^n[W]$ is isomorphic to $P_p^n[W(a)]$.

Proof

Let Ψ be a mapping such that for $a \in P_p^n[W(a)]$,

$$\Psi(a) = W \in M_p^n[W]$$

$$\text{Let } q(a) = \sum_{i=0}^{n-1} q_i a^i \quad \text{and} \quad g(a) = \sum_{i=0}^{n-1} g_i a^i \in P_p^n[W(a)]$$

$$\text{we have } \Psi(q(a)) = \Psi\left(\sum_{i=0}^{n-1} q_i a^i\right) = \sum_{i=0}^{n-1} q_i W^i \quad \text{and}$$

$$\begin{aligned} \text{(i) } \Psi(q(a)+g(a)) &= \Psi\left(\sum_{i=0}^{n-1} (q_i+g_i) a^i\right) = \sum_{i=0}^{n-1} (q_i+g_i) W^i \\ &= \sum_{i=0}^{n-1} q_i W^i + \sum_{i=0}^{n-1} g_i W^i = \Psi(q(a)) + \Psi(g(a)). \end{aligned}$$

$$\text{(ii) } \Psi(q(a).g(a)) = \Psi\left(\sum_{i=0}^{n-1} q_i a^i \sum_{j=0}^{n-1} g_j a^j\right) = \Psi\left(\sum_{k=0}^{n-1} h_k a^k\right);$$

$$\text{where } h_k = \sum_{i+j=k} q_i g_j$$

This is equal to $\sum_{k=0}^{n-1} h_k W^k = (\sum_i q_i W^i)(\sum_j g_j W^j) = \Psi(q(a)) \Psi(g(a))$

(iii) $\Psi(1) = I$ $n \times n$ identity matrix.

From (i), (ii) and (iii) we see that

Ψ satisfies the properties of a ring homomorphism .

Now suppose $\Psi(q(a)) = \underline{0}$

That is $\sum_{i=0}^{n-1} q_i W^i = \underline{0}$ ($n \times n$ null matrix) .

From the result of Lemma 2.6.1 this implies $q_i = 0$ for all $i = 0, \dots, n-1$, therefore, only $0 \in P_p^n[W(a)]$ is mapped to $\underline{0} \in M_p^n[W]$. That is $\text{Ker } \Psi = 0$. Thus Ψ is one to one and since the order of the two rings are same Ψ is onto. Hence Ψ is an isomorphism.

The elements of the ring $M_p^n[W]$ are of the form

$Q = \sum_{i=0}^{n-1} q_i W^i$ and the inverse mapping Ψ^{-1} is defined as

$$\Psi^{-1}: W \rightarrow a \text{ and } \Psi^{-1}(Q) = \Psi^{-1}\left(\sum_{i=0}^{n-1} q_i W^i\right) = \sum_{i=0}^{n-1} q_i a^i = q(a).$$

*

Example 2.6.1

Consider $P_2^2[a^2+1] = \{0, 1, a, 1+a\}$.

$$W = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Hence we have $1 \xrightarrow{\sim} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; $a \xrightarrow{\sim} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$; $(1+a) \xrightarrow{\sim} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$; $0 \xrightarrow{\sim} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

The 2×2 matrices are the elements of M_2^2 . The operations in $P_2^2[a^2+1]$ are polynomial addition and multiplication modulo $[2; a^2+1]$. The operations in the ring $M_2^2 \simeq P_2^2[a^2+1]$ are matrix addition and multiplication modulo 2.

Example 2.6.2

Consider $P_2^3[a^3+a^2+a+1]$. The elements of this ring are = $\{0, 1, a, a^2, 1+a, 1+a^2, a+a^2, 1+a+a^2\}$. The operations are polynomial addition and multiplication modulo $[2; a^3+a^2+a+1]$.

$$W = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

With the correspondence $a^i \xrightarrow{\sim} W^i$ the elements of the corresponding commutative ring M_2^3 of matrices are

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \\ \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

The operations are matrix addition and multiplication modulo 2.

*

Example 2.6.3

Consider $P_3^2[a^2-1]$. The elements of this ring are $\{0, 1, 2, a, 2a, 1+a, 2+a, 1+2a, 2+2a\}$. The operations are polynomial addition and multiplication modulo $[3, a^2-1]$.

$$W = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

With the correspondence $ja^i \rightarrow jW^i$ the elements of the corresponding commutative ring M_3^2 of matrices are

$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \right. \\ \left. \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \right\}.$$

*

The operations are matrix addition and multiplication modulo 3.

Now we give two procedures for constructing the individual elements $Q \in M_p^n[W] \simeq P_{p^{n-1}}^n[W(a)]$. Towards this end we will show that in the matrix $Q = \sum_{i=0}^{n-1} q_i W^i$, $q_i \in GF(p)$, the zeroth column determines the remaining columns. First we prove the following lemma.

Lemma 2.6.3

If W is the $n \times n$ companion matrix of the modulus polynomial $W(a)$ of degree n , then in the set of $n \times n$ matrices $\{W^0 \triangleq I, W, W^2, \dots, W^{n-1}\}$, the j th column of the matrix $W^i, i=0, 1, \dots, n-1$

is equal to the column vector of coefficients of a^{i+j} modulo $[p; W(a)]$, $j = 0, 1, \dots, n-1$.

Proof

Consider W^0 . The j th column of this matrix \underline{a}^j is the column vector of coefficients of a^j modulo $[p; W(a)]$.

The j th column of W which we denote by \underline{a}^{j+1} is the column vector of coefficients of a^{j+1} modulo $[p; W(a)]$.

The j th column of W^2 which we denote by \underline{a}^{j+2} , is the column vector of coefficients of a^{j+2} modulo $[p; W(a)]$.

In general the j th column of W^i , which we denote by \underline{a}^{j+i} , is the column vector of coefficients of a^{j+i} modulo $[p; W(a)]$.

Now we prove the following theorem which gives a construction procedure for obtaining Q given $q(a) \in P_p^n[W(a)]$. *

Theorem 2.6.3

Let $q(a) = \sum_{i=0}^{n-1} q_i a^i \in P_p^n[W(a)]$ then the j th column Q_j of $Q = \sum_{i=0}^{n-1} q_i W^i$ is given by the column vector of coefficients $a^j q(a)$ modulo $[p; W(a)]$.

Proof :

$$Q = \sum_{i=0}^{n-1} q_i W^i$$

$$\underline{Q}_j = \sum_{i=0}^{n-1} q_i \begin{bmatrix} \text{jth} \\ \text{Column of} \\ W^i \end{bmatrix}$$

$$= \text{column vector of coefficients of } \sum_{i=0}^{n-1} q_i [a^{j+i} \text{ modulo}[p; W(a)]]$$

$$= \quad '' \quad '' \quad a^j \sum_{i=0}^{n-1} q_i [a^i \text{ modulo}[p; W(a)]]$$

$$= \quad '' \quad '' \quad a^j q(a) \text{ modulo}[p; W(a)] .$$

Zeroth column is the column vector of coefficients of $q(a)$ modulo $[p; W(a)] = q(a)$.

Computation of $aq(a) \text{ modulo}[p; W(a)]$ can be carried out as a vector matrix multiplication as indicated in [8,12,13].

We have

$$q(a) = \sum_{i=0}^{n-1} q_i a^i = q_0 + q_1 a + \dots + q_{n-1} a^{n-1}$$

$$aq(a) = q_0 a + q_1 a^2 + \dots + q_{n-2} a^{n-1} + q_{n-1} a^n$$

$$aq(a) \text{ mod}[p; W(a)] = q_0 a + q_1 a^2 + \dots + q_{n-2} a^{n-1} - q_{n-1} (w_0 + w_1 a + \dots + w_{n-1} a^{n-1})$$

$$= -q_{n-1} w_0 + (q_0 - q_{n-1} w_1) a + (q_1 - q_{n-1} w_2) a^2 + \dots + (q_{n-2} - q_{n-1} w_{n-1}) a^{n-1} .$$

The column vector of coefficients of $aq(a) \text{ mod}[p; W(a)]$ is

$$= \begin{bmatrix} -q_{n-1} w_0 \\ q_0 -q_{n-1} w_1 \\ q_1 -q_{n-1} w_2 \\ \vdots \\ q_{n-2} -q_{n-1} w_{n-1} \end{bmatrix} \triangleq q'$$

Now let us consider the product $W_q Wq$

$$W_q = \begin{bmatrix} 0 & 0 & 0 & \dots & -w_0 \\ 1 & 0 & 0 & \dots & -w_1 \\ 0 & 1 & 0 & \dots & -w_2 \\ 0 & 0 & 1 & \dots & -w_3 \\ \vdots & & & & \\ 0 & 0 & 0 & & -w_{n-1} \end{bmatrix} \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{bmatrix} = \begin{bmatrix} -q_{n-1} w_0 \\ q_0 -q_{n-1} w_1 \\ q_1 -q_{n-1} w_2 \\ \vdots \\ q_{n-2} -q_{n-1} w_{n-1} \end{bmatrix} = q'$$

Thus multiplication of $q(a)$ by a and finding remainder after division by $q(a)$ can be achieved by the multiplication of matrix W and vector q . In other words $aq(a) \equiv Wq$ and it follows that

$$a^j q(a) \equiv W^j q$$

*

Now we prove the following theorem which gives another construction procedure for obtaining Q given $q(a) \in P_p^n[W(a)]$.

Theorem 2.6.4

Let $q(a) \in P_p^n[W(a)]$. Let Q_0 be the zeroth column in the

matrix $Q \in M_p^n[W]$. Then the j th column of matrix Q is given by $W^j \underline{Q}_0 = W \underline{Q}_{j-1}$, $j = 1, 2, \dots, n-1$; $\underline{Q}_0 = q$.

Proof

From the result of Theorem 2.6.3 we have \underline{Q}_0 , zeroth column of Q = column vector of coefficients of $q(a) = q$.

$$\begin{aligned} \underline{Q}_1 \quad \text{1st column of } Q &= \text{column vector of coefficients of } aq(a) : \\ &= W q = W \underline{Q}_0 \end{aligned}$$

$$\begin{aligned} \underline{Q}_2 \quad \text{2nd column of } Q &= \text{column vector of coefficients of } a^2 q(a) \\ &= W^2 \underline{Q}_0 = W \underline{Q}_1 \end{aligned}$$

Continuing it can be shown that

$$\underline{Q}_j, j\text{th column of } Q = W^j \underline{Q}_0 = W \underline{Q}_{j-1}. \quad *$$

Given $q(a) = \sum_{i=0}^{n-1} q_i a^i \in P_p^n[W(a)]$; Theorems 2.6.3 and

2.6.4 specify two procedures for obtaining $Q \in M_p^n[W] \simeq P_p^n[W(a)]$.

These may be summarised as follows.

Procedure 1

The zeroth column of Q is the column vector of coefficients of $q(a)$,

$$\begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{bmatrix}$$

and the j th column is the column vector of coefficients of $a^j q(a) \bmod[p; W(a)]$.

Procedure 2

The zeroth column of Q is $Q_0 = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{bmatrix}$ and the j th column is $W^j Q_0 = W Q_{j-1}; \quad j = 1, 2, \dots, n-1.$

The following example illustrates the procedure for constructing Q given $q(a) \in P_2^3[a^3+a+1]$.

Example 2.6.4

Let $(a^2+a) \in P_2^3[a^3+a+1]$.

The corresponding 3×3 matrix in the commutative ring of 3×3 matrices isomorphic to $P_2^3[a^3+a+1]$ is obtained as follows.

Procedure 1

We consider the three polynomials

$$(a^2+a), (a^2+a)a, (a^2+a)a^2$$

these are written as elements of residue class polynomial ring $P_2^3[a^3+a+1]$.

$$(a^2+a), (a^3+a^2) = (a^2+a+1), \quad a^4+a^3 = a^2+1$$

The matrix corresponding to (a^2+a) is obtained by writing the three polynomials in column vector form.

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

Procedure 2

We have $W = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ and $(a^2+a) \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$

The matrix \underline{Q} corresponding to (a^2+a) has $\underline{Q}_0 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$

The remaining column can be computed as follows.

$$\underline{Q}_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$\underline{Q}_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$(a^2+a) \cdot \underline{Q} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

Procedure 2 is simpler than Procedure 1.

The ring $M_p^n[W]$ of $n \times n$ matrices isomorphic to $P_p^n[a^n-1]$ is a commutative ring of $n \times n$ cyclic matrices over $GF(p)$. The order of the ring is p^n . In each matrix the successive columns are the cyclic shift of the first column.

Now we obtain a ring of nxn matrices isomorphic to a given $\bigotimes_{i=0}^r \{P_p^{n_i}[W_i(a_i)]\}$

2.6.2 Ring $\bigotimes_{i=0}^r \{M_p^{n_i}[W_i]\}$ of nxn Matrices Over GF(p) Isomorphic to $\bigotimes_{i=0}^r \{P_p^{n_i}[W_i(a_i)]\}$

We will see that this case is an extension of the case discussed in Subsection 2.6.1. The ring of nxn matrices isomorphic to $\bigotimes_{i=0}^r \{P_p^{n_i}[W_i(a_i)]\}$ will be shown to be a linear combination of a set of Kronecker products of matrices [Appendix C] obtained in the single variable case discussed in Subsection 2.6.1. We first consider the case $r = 2$.

Consider the tensor product of two residue class polynomial rings $P_p^{n_1}[W_1(a_1)]$ and $P_p^{n_0}[W_0(a_0)]$ of order p^{n_1} and p^{n_0} respectively. The tensor product $P_p^{n_1}[W_1(a_1)] \bigotimes P_p^{n_0}[W_0(a_0)]$ is a ring of order p^n , where $n = n_1 n_0$. In this tensor product ring the elements are polynomials in two variables a_1 and a_0 . The ring elements of the form $a_1^{i_1} a_0^{i_0}$, with $0 \leq i_1 \leq (n_1-1)$ and $0 \leq i_0 \leq (n_0-1)$, are linearly independent and constitute a basis of the tensor product ring.

We show below that it is possible to obtain a ring of nxn matrices over GF(p) which is isomorphic to $P_p^{n_1}[W_1(a_1)] \bigotimes P_p^{n_0}[W_0(a_0)]$.

Let W_1 and W_0 be companion matrices of $W_1(a_1)$ and $W_0(a_0)$ respectively. From the results of Subsection 2.6.1

$$\{W_1^0, W_1^1, W_1^2, \dots, W_1^{n_1-1}\} \quad (2.6.3)$$

and

$$\{W_0^0, W_0^1, W_0^2, \dots, W_0^{n_0-1}\} \quad (2.6.4)$$

are respectively the sets of $n_1 \times n_1$ and $n_0 \times n_0$ linearly independent matrices. The set of all linear combination of (2.6.3) constitute the commutative ring $M_p^{n_1}[W_1]$ of $n_1 \times n_1$ matrices isomorphic to $P_p^{n_1}[W_1(a_1)]$. The set of all linear combination of (2.6.4) constitute the commutative ring $M_p^{n_0}[W_0]$ of $n_0 \times n_0$ matrices isomorphic to $P_p^{n_0}[W_0(a_0)]$.

Let $a_1 \in P_p^{n_1}[W_1(a_1)]$ and $a_0 \in P_p^{n_0}[W_0(a_0)]$

We apply the correspondences $a_1 \rightleftharpoons W_1$ and $a_0 \rightleftharpoons W_0$ discussed in Subsection 2.6.1 in two stages. Using $a_1 \rightleftharpoons W_1$ we have,

$$a_1 a_0 \rightleftharpoons W_1 a_0 \quad \text{where we treat } a_0 \text{ fixed.}$$

Expanding the matrix W_1 we have

$$W_1 a_0 = \begin{bmatrix} W_{1_{00}} & W_{1_{01}} & \dots & W_{1_{0n_1-1}} \\ W_{1_{n_1-1,0}} & W_{1_{n_1-1,1}} & \dots & W_{1_{n_1-1,n_1-1}} \end{bmatrix} a_0$$

Taking a_0 inside we have,

$$W_1 a_0 = \begin{bmatrix} w_{1,0,0} a_0 & w_{1,0,1} a_0 & \dots & w_{1,0,n_1-1} a_0 \\ \vdots & & & \vdots \\ w_{1,n_1-1,0} a_0 & w_{1,n_1-1,1} a_0 & \dots & w_{1,n_1-1,n_1-1} a_0 \end{bmatrix} \quad (2.6.5)$$

Now we apply the correspondence $a_0 \rightarrow W_0$ and we have

$$a_1 a_0 \rightarrow \begin{bmatrix} w_{1,0,0} W_0 & w_{1,0,1} W_0 & \dots & w_{1,0,n_1-1} W_0 \\ \vdots & & & \vdots \\ w_{1,n_1-1,0} W_0 & w_{1,n_1-1,1} W_0 & \dots & w_{1,n_1-1,n_1-1} W_0 \end{bmatrix} \quad (2.6.6)$$

where $w_{1,j}$ is an element of matrix W_1 and is from $GF(p)$ while W_0 is $n_0 \times n_0$ matrix over $GF(p)$. This matrix is symbolically represented as $W_1 \otimes W_0$ and is called the Kronecker product of matrices W_1 and W_0 . The properties of Kronecker product of matrices which are relevant here have been given in Appendix C.

In general $W_1 \otimes W_0$ is not equal to $W_0 \otimes W_1$.

$$\text{We can see that } a_1^{i_1} a_0^{i_0} \Rightarrow W_1^{i_1} \otimes W_0^{i_0} \quad (2.6.7)$$

Since powers of W_i ; $i = 0, 1$ commute, the Kronecker products of the form (2.6.7) are commutative. That is ,

$$\begin{aligned}
(W_1^{j_1} \otimes W_0^{j_0})(W_1^{i_1} \otimes W_0^{i_0}) &\triangleq (W_1^{j_1} W_1^{i_1} \otimes W_0^{j_0} W_0^{i_0}) \\
&= (W_1^{i_1} W_1^{j_1} \otimes W_0^{i_0} W_0^{j_0}) = (W_1^{i_1} \otimes W_0^{i_0})(W_1^{j_1} \otimes W_0^{j_0})
\end{aligned}$$

Consider the set of matrices

$$\begin{array}{ccccccc}
W_1^0 \otimes W_1^0, & W_1^0 \otimes W_0, & W_1^0 \otimes W_0^2, & \dots & W_1^0 \otimes W_0^{n_0-1} \\
W_1^1 \otimes W_0^0, & W_1^1 \otimes W_0, & W_1^1 \otimes W_0^2, & \dots & W_1^1 \otimes W_0^{n_0-1} \\
W_1^2 \otimes W_0^0, & W_1^2 \otimes W_0, & W_1^2 \otimes W_0^2, & \dots & W_1^2 \otimes W_0^{n_0-1} \\
\vdots & & & & \vdots \\
W_1^{n_1-1} \otimes W_0^0, & W_1^{n_1-1} \otimes W_0, & W_1^{n_1-1} \otimes W_0^2, & \dots & W_1^{n_1-1} \otimes W_0^{n_0-1}
\end{array}$$

(2.6.8)

This set of $n_1 n_0 = n$ matrices, each of size $n \times n$, is linearly independent and linear combinations of these matrices constitutes a tensor product of commutative matrix rings $M_{p^1}^{n_1}[W_1]$ and $M_p^{n_0}[W_0]$. We denote this tensor product by $M_p^{n_1}[W_1] \otimes M_p^{n_0}[W_0]$ which is a commutative ring of order p^n . The operations in this ring are the usual matrix addition and multiplication modulo p .

Having seen that, corresponding to element

$a_1 a_0 \in P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]$, there is an $n \times n$ matrix $W_1 \otimes W_0$ and the existence of tensor product rings of commutative

matrices, $M_p^{n_1}[W_1]$ and $M_p^{n_0}[W_0]$, we now prove the following theorem.

Theorem 2.6.5

$$M_p^{n_1}[W_1] \otimes^T M_p^{n_0}[W_0] \simeq P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)] .$$

Proof

$$\text{Let } q(a_1, a_0) = \sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} q_{i_1, i_0} a_1^{i_1} a_0^{i_0} \in P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)] \quad (2.6.9)$$

Then from the correspondence (2.6.5) we have

$$q(a_1, a_0) \simeq \sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} q_{i_1, i_0} W_1^{i_1} \otimes W_0^{i_0} = Q \quad (2.6.10)$$

From (2.6.8) we see that the right hand side of the correspondence (2.6.10) is an element of $M_p^{n_1}[W_1] \otimes^T M_p^{n_0}[W_0]$.

Since right hand side of the correspondence (2.6.10) is a linear combination of linearly independent matrices, $Q = \underline{0}$ implies that the coefficients $q_{i_1, i_0} = 0$, $\forall i_1, i_0$. Therefore, only zero of $P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}(a_0)]$ is mapped to null matrix. Therefore, if Ψ represents the mapping from tensor product polynomial ring to tensor product matrix ring, then Kernel of Ψ is zero. This implies Ψ is one to one. Thus,

(i) for each element in $P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)]$ there is a unique matrix in $M_p^{n_1}[W_1] \otimes^T M_p^{n_0}[W_0]$.

(ii) the order of the two rings are same.

Hence they are isomorphic.

Every element of $M_p^{n_1}[W_1] \otimes^T M_p^{n_0}[W_0]$ is of the form

$$Q = \sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} q_{i_1 i_0} W_1^{i_1} \otimes W_0^{i_0}$$

The inverse mapping Ψ^{-1} is defined as

$$\Psi^{-1}: W_1^{i_1} \otimes W_0^{i_0} \rightarrow a_1^{i_1} a_0^{i_0}$$

and

$$\Psi^{-1}(Q) = \Psi^{-1} \sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} q_{i_1 i_0} W_1^{i_1} \otimes W_0^{i_0} = \sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} q_{i_1 i_0} a_1^{i_1} a_0^{i_0}$$

The operations in $M_p^{n_1}[W_1] \otimes^T M_p^{n_0}[W_0]$, the ring of $n \times n$ commutative matrices as stated earlier are the usual operations of addition and multiplication modulo p of matrices.

*

Example 2.6.5

Consider $P_2^2[a_1^2+1] \otimes^T P_2^2[a_0^2+a_0+1]$. Elements of this residue class ring of polynomials are of the form

$$q_{00} + q_{01}a_0 + q_{10}a_1 + q_{11}a_1a_0, \quad q_{ij} \in GF(2)$$

which can be considered as a linear combination of the basis elements

$$\{1, a_0, a_1, a_1 a_0\} \quad (2.6.11)$$

We have $W_0 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ and $W_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

The correspondence between the elements given in Equation (2.6.11) and the 4x4 matrices are

$$\begin{aligned} 1 &\approx W_1^0 \otimes W_0^0 = I_2 \otimes I_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\ a_0 &\approx W_1^0 \otimes W_0 = I_2 \otimes W_0 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \\ a_1 &\approx W_1 \otimes W_0^0 = W_1 \otimes I_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \\ a_1 a_0 &\approx W_1 \otimes W_0 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \end{aligned} \quad (2.6.12)$$

The linear combinations of the matrices given in Equation (2.6.12) constitute the ring of 4×4 commutative binary matrices isomorphic to $P_2^2[a_1^2+1] \otimes^T P_2^2[a_0^2+a_0+1]$. Thus corresponding to the polynomial $q(a_1, a_0) = 1 + a_0 + a_1 a_0 \in P_2^2[a_1^2+1] \otimes^T P_2^2[a_0^2+a_0+1]$ we have

$$\text{the matrix } Q = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

*

Example 2.6.6

Consider $P_2^2[a_1^2+1] \otimes^T P_2^3[a_0^3+1]$ the elements of this ring are linear combinations of $\{1, a_0, a_0^2, a_1, a_1 a_0, a_1 a_0^2\}$ we have

$$W_0 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad W_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and}$$

the corresponding 6×6 matrices are

$$1 \approx W_1^0 \otimes W_0^0 = I_2 \otimes I_3, \quad a_0 \approx W_1^0 \otimes W_0^1 = I_2 \otimes W_0,$$

$$a_0^2 \approx W_1^0 \otimes W_0^2 = I_2 \otimes W_0^2$$

$$a_1 \approx W_1^1 \otimes W_0^0 = W_1 \otimes I_3, \quad a_1 a_0 \approx W_1^1 \otimes W_0^1, \quad a_1 a_0^2 \approx W_1^1 \otimes W_0^2$$

(2.6.13)

The linear combinations of the matrices given in (2.6.13) constitute the 6x6 commutative ring of binary matrices isomorphic to

$P_2^2[a_1^2+1] \otimes^T P_2^3[a_0^3+1]$. Thus corresponding to polynomial $q(a_1 a_0) = 1 + a_1 a_0 \in P_2^2[a_1^2+1] \otimes^T P_2^3[a_0^3+1]$, we have the matrix

$$Q = I_2 \otimes I_3 + W_1 \otimes W_0 = \begin{bmatrix} 1 & 0 & 0 & | & 0 & 0 & 1 \\ 0 & 1 & 0 & | & 1 & 0 & 0 \\ 0 & 0 & 1 & | & 0 & 1 & 0 \\ \hline 0 & 0 & 1 & | & 1 & 0 & 0 \\ 1 & 0 & 0 & | & 0 & 1 & 0 \\ 0 & 1 & 0 & | & 0 & 0 & 1 \end{bmatrix}$$

*

Having shown that there exists an isomorphism between the tensor product rings, $P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)]$ and

$M_p^{n_1}[W_1] \otimes^T M_p^{n_0}[W_0]$, we will now give two procedures for obtaining individual elements of tensor product ring of matrices. Given $q(a_1 a_0)$, an element of tensor product of residue class polynomial ring, we obtain the corresponding nxn matrix Q which is an element of tensor product of commutative rings of matrices. Towards this end we first show that in the matrix Q the j th column is determined by $q(a_1 a_0)$, $W_1(a_1)$ and $W_0(a_0)$ or alternatively by $q(a_1 a_0)$, W_1 and W_0 . Let $W = W_1 \otimes W_0$. The ij th element of W is given by (Appendix C).

$$W_{ij} = W_{\langle i_1 i_0 \rangle \langle j_1 j_0 \rangle} = W_{1 i_1 j_1} \cdots W_{0 i_0 j_0}$$

where $W_{1 i_1 j_1}$ is the $i_1 j_1$ th element of W_1 , and $W_{0 i_0 j_0}$ is the $i_0 j_0$ th element of W_0 .

$\langle i_1 i_0 \rangle$, $\langle j_1 j_0 \rangle$ are the mixed radix representations (Appendix B) of integers i and j respectively with mixed radices n_0 and n_1 . The j th column of the matrix W is a $(n_1 n_0 \times 1)$ vector.

$$\begin{bmatrix} W_{1 0 j_1} \cdot W_{0 0 j_0} \\ W_{1 0 j_1} \cdot W_{0 1 j_0} \\ \cdot \cdot \cdot \cdot \\ W_{1 0 j_1} \cdot W_{0 n_0 - 1, j_0} \\ \\ W_{1 1 j_1} \cdot W_{0 0 j_0} \\ \cdot \cdot \cdot \cdot \\ W_{1 1 j_1} \cdot W_{0 1 j_0} \\ \cdot \cdot \cdot \cdot \\ W_{1 1 j_1} \cdot W_{0 n_0 - 1, j_0} \\ \\ W_{1 n_1 - 1, j_1} \cdot W_{0 0 j_0} \\ W_{1 n_1 - 1, j_1} \cdot W_{0 1 j_0} \\ W_{1 n_1 - 1, j_1} \cdot W_{0 n_0 - 1, j_0} \end{bmatrix} \quad (2.6.14)$$

This can be written in short form as the Kronecker product

$$\underline{W}_{j_1} \otimes \underline{W}_{j_0}$$

where \underline{W}_1 is the j_1 th column of W_1

and \underline{W}_0 is the j_0 th column of W_0 .

We consider the following examples which illustrates the determination of columns of W .

Example 2.6.7

Consider $P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]$,

where $W_1(a_1) = \omega_{10} + \omega_{11}a_1 + \omega_{12}a_1^2 + a_1^3$

$$W_0(a_0) = \omega_{00} + \omega_{01}a_0 + a_0^2$$

Companion matrix of $W_1(a_1)$ is

$$W_1 = \begin{bmatrix} 0 & 0 & -\omega_{10} \\ 1 & 0 & -\omega_{11} \\ 0 & 1 & -\omega_{12} \end{bmatrix}$$

Companion matrix of $W_0(a_0)$ is

$$W_0 = \begin{bmatrix} 0 & -\omega_{00} \\ 1 & -\omega_{01} \end{bmatrix}$$

We have

$$W = W_1 \otimes W_0 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & \omega_{10}\omega_{00} \\ 0 & 0 & 1 & 0 & 0 & 1 & -\omega_{10} & \omega_{10}\omega_{01} \\ 0 & -\omega_{00} & 0 & 0 & 0 & 0 & 0 & \omega_{11}\omega_{00} \\ 1 & -\omega_{01} & 0 & 0 & 0 & 1 & -\omega_{11} & \omega_{11}\omega_{01} \\ 0 & 0 & 0 & 0 & -\omega_{00} & 0 & 0 & \omega_{12}\omega_{00} \\ 0 & 0 & 1 & -\omega_{01} & -\omega_{12} & 0 & 0 & \omega_{12}\omega_{01} \end{bmatrix} \quad (2.6.15)$$

In this example degree of $W_1(a_1) = n_1 = 3$

and degree of $W_0(a_0) = n_0 = 2$

The mixed radices are 3 and 2 (Appendix B).

Using the mixed radix representation of integers 0, 1, ..., 5 we find that the columns of W are Kronecker product of appropriate columns of W_1 and W_0 .

The integers 0, 1, ..., 5 and their mixed radix representations are given below.

$i = 2i_1 + i_0$	$\langle i_1 i_0 \rangle$; $0 \leq i_1 < 3$; $0 \leq i_0 < 2$
0	$\langle 0 0 \rangle$
1	$\langle 0 1 \rangle$
2	$\langle 1 0 \rangle$
3	$\langle 1 1 \rangle$
4	$\langle 2 0 \rangle$
5	$\langle 2 1 \rangle$

(2.6.16)

An element $q(a_1, a_0) \in P_p^3[W_1(a_1)] \otimes^T P_p^2[W_0(a_0)]$, which is a polynomial in the two variables a_1 and a_0 is written in the following order.

$$q(a_1, a_0) = q_{00}a_1^0a_0^0 + q_{01}a_1^0a_0^1 + q_{10}a_1^1a_0^0 + q_{11}a_1^1a_0^1 + q_{20}a_1^2a_0^0 + q_{21}a_1^2a_0^1;$$

$$q_{i_1, i_0} \in GF(p).$$

We note here that the index $\langle i_1 i_0 \rangle$ of the coefficient $q_{i_1 i_0}$ is also the power of a_1 and a_0 respectively and is in the ascending order of the mixed radix representation of integers. Now, we write the columns of matrix W .

Zeroth column \underline{W}_0 of W : Since $0 \rightarrow \langle 0 0 \rangle$, \underline{W}_0 is equal to the Kronecker product of zeroth columns, $\underline{W}1_0$ of W_1 and $\underline{W}0_0$ of W_0

$$\underline{W}1_0 \otimes \underline{W}0_0 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

which is equal to the column vector of coefficients of $a_1 a_0$. First column \underline{W}_1 of W : Since $1 \rightarrow \langle 0 1 \rangle$, \underline{W}_1 is equal to the Kronecker product of zeroth column $\underline{W}1_0$ of W_1 and first column $\underline{W}0_1$ of W_0

$$\underline{W}1_0 \otimes \underline{W}0_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} -w_{00} \\ -w_{01} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -w_{00} \\ -w_{01} \\ 0 \\ 0 \end{bmatrix}$$

which is equal to the column vector of coefficients of $a_1 a_0^2$ modulo $[p; W_1(a_1), W_0(a_0)]$.

Second column \underline{W}_2 of W : Since $2 \rightarrow \langle 1 \ 0 \rangle$,

$$\underline{W}_2 = \underline{W}1_1 \otimes \underline{W}0_0 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

which is equal to the column vector of coefficients of $a_1^2 a_0$ modulo $[p; W_1(a_1), W_0(a_0)]$.

Third column \underline{W}_3 of W : Since $3 \rightarrow \langle 1 \ 1 \rangle$

$$\underline{W}_3 = \underline{W}1_1 \otimes \underline{W}0_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} -\omega_{00} \\ -\omega_{01} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ -\omega_{00} \\ -\omega_{01} \end{bmatrix}$$

which is equal to the column vector of coefficients of $a_1^2 a_0^2$ modulo $[p; W_1(a_1), W_0(a_0)]$.

Fourth column \underline{W}_4 of W : Since $4 \rightarrow \langle 2, 0 \rangle$

$$\underline{W}_4 = \underline{W}_{12} \otimes \underline{W}_{00} = \begin{bmatrix} -\omega_{10} \\ -\omega_{11} \\ -\omega_{12} \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -\omega_{10} \\ 0 \\ -\omega_{11} \\ 0 \\ -\omega_{12} \end{bmatrix}$$

which is equal to the column vector of coefficients of $a_1^3 a_0$ modulo $[p; W_1(a_1), W_0(a_0)]$.

Fifth column \underline{W}_5 of W : Since $5 \rightarrow \langle 2, 1 \rangle$

$$\underline{W}_5 = \underline{W}_{12} \otimes \underline{W}_{01} = \begin{bmatrix} -\omega_{10} \\ -\omega_{11} \\ -\omega_{12} \end{bmatrix} \otimes \begin{bmatrix} -\omega_{00} \\ -\omega_{01} \end{bmatrix} = \begin{bmatrix} \omega_{10} \omega_{00} \\ \omega_{10} \omega_{01} \\ \omega_{11} \omega_{00} \\ \omega_{11} \omega_{01} \\ \omega_{12} \omega_{00} \\ \omega_{12} \omega_{01} \end{bmatrix}$$

which is equal to the column vector of coefficients of $a_1^3 a_0^2 \bmod [p; W_1(a_1), W_0(a_0)]$.

Now we take up the procedures for obtaining j th column $\underline{\Omega}_j$ of $Q \in M_p^{n_1}[W_1] \otimes M_p^{n_0}[W_0]$ corresponding to

$$\sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} a_1^{i_1} a_0^{i_0} \in P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]^T.$$

We have $\underline{Q} = \sum_{i_1} \sum_{i_0} q_{i_1 i_0} W_1^{i_1} \otimes W_0^{i_0}$

$$\underline{Q}_0 = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} \begin{bmatrix} \text{zeroth column} \\ \text{of } W_1^{i_1} \end{bmatrix} \otimes \begin{bmatrix} \text{zeroth column} \\ \text{of } W_0^{i_0} \end{bmatrix}$$

Using the results of Example 2.6.7

$$\underline{Q}_0 = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} \begin{bmatrix} \text{column vector of coefficients} \\ a_1^{i_1} a_0^{i_0} \bmod [p; W_1(a_1), W_0(a_0)] \end{bmatrix}$$

$$= \text{column vector of coefficients of } \sum_{i_1} \sum_{i_0} q_{i_1 i_0} a_1^{i_1} a_0^{i_0}$$

$$= \text{column vector of coefficients of } q(a_1 a_0)$$

$$= \begin{bmatrix} q_{0,0} \\ q_{0,1} \\ \vdots \\ q_{0,n_0-1} \\ q_{1,0} \\ q_{1,1} \\ \vdots \\ q_{1,n_0-1} \\ q_{i_1,i_0} \\ q_{(n_1-1),0} \\ q_{(n_1-1),1} \\ \vdots \\ q_{(n_1-1),(n_0-1)} \end{bmatrix} = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_i \\ q_{n-1} \end{bmatrix} = q$$

where $q_i \triangleq q_{i_1 i_0}$

and $\langle i_1 i_0 \rangle$ is the mixed radix number system representation of the integer i with respect to mixed radices n_0 and n_1 . Thus we see that $q \neq q(a_1 a_0)$.

Now consider the j th column Q_j of Q we have

$$Q_j = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} \quad [j\text{th column of } W_1^{i_1} \otimes W_0^{i_0}] \quad (2.6.17)$$

$$= \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} \quad [j_1\text{th column of } W_1^{i_1}] \otimes [j_0\text{th column of } W_0^{i_0}] \quad (2.6.18)$$

From the result of Lemma 2.6.3 we have, j_1 th column of $W_1^{i_1}$ = column vector of coefficients of $a_1^{j_1+i_1}$ and j_0 th column of $W_0^{i_0}$ = column vector of coefficients of $a_0^{j_0+i_0}$. Hence from Equation (2.6.18) and Example 2.6.7

$$Q_j = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} \left[\begin{array}{c} \text{column vector of coefficients of} \\ (a_1^{j_1+i_1} a_0^{j_0+i_0}) \text{ modulo}[p; W_1(a_1), W_0(a_0)] \end{array} \right]$$

Bringing $a_1^{j_1} a_0^{j_0}$ outside the summation we have,

$$\begin{aligned} Q_j &= \text{column vector of coefficients of} \\ &\left[\begin{array}{c} a_1^{j_1} a_0^{j_0} \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} a_1^{i_1} a_0^{i_0} \text{ modulo}[p; W_1(a_1), W_0(a_0)] \end{array} \right] \\ &= \text{column vector of coefficients of } [a_1^{j_1} a_0^{j_0} q(a_1 a_0)] \\ &\quad \text{modulo}[p; W_1(a_1), W_0(a_0)] \quad (2.6.19) \end{aligned}$$

Hence given $q(a_1, a_0)$, $W_1(a_1)$ and $W_0(a_0)$, the columns of the corresponding matrix Q can be obtained from (2.6.19).

The matrix Q can also be obtained alternatively as discussed below.

From Theorem 2.6.4, we have,

$$j_1 \text{th column of } W_1^{i_1} = W_1^{j_1} [\text{zeroth column of } W_1^{i_1}] = W_1^{j_1} W_1^{i_1} \text{ and}$$

$$j_0 \text{th column of } W_0^{i_0} = W_0^{j_0} [\text{zeroth column of } W_0^{i_0}] = W_0^{j_0} W_0^{i_0}$$

Therefore from Equation (2.6.18)

$$Q_j = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} [(W_1^{j_1} W_1^{i_1}) \otimes (W_0^{j_0} W_0^{i_0})] \quad (2.6.20)$$

Using the property

$$PP' \otimes RR' = (P \otimes R) (P' \otimes R')$$

of Kronecker product of matrices we have

$$Q_j = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} [(W_1^{j_1} \otimes W_0^{j_0}) (W_1^{i_1} \otimes W_0^{i_0})]$$

Since the summation is over i_1 and i_0 we can bring $W_1^{j_1} \otimes W_0^{j_0}$ outside the summation,

$$Q_j = [W_1^{j_1} \otimes W_0^{j_0}] \left[\sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} (W_1^{i_1} \otimes W_0^{i_0}) \right].$$

Using the result of Lemma 2.6.3 and from the Example 2.6.7

$$Q_j = [W_1^{j_1} \otimes W_0^{j_0}] [\text{column vector of coefficients of } q(a_1 a_0)] \quad (2.6.21)$$

$$Q_j = [W_1^{j_1} \otimes W_0^{j_0}] q$$

Hence given $q(a_1 a_0)$, $W_1(a_1)$, and $W_0(a_0)$, the column of the corresponding matrix Q can be obtained from (2.6.21).

To summarise we have the following two procedures for obtaining $Q \in M_p^{n_1}[W_1] \otimes M_p^{n_0}[W_0]$ corresponding to

$$q(a_1 a_0) \in P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)].$$

Procedure 1

Given $q(a_1 a_0)$ compute $a_1^{j_1} a_0^{j_0} q(a_1 a_0) \text{ modulo } [p; W_1(a_1), W_0(a_0)]$
 $j_i = 0, 1 \dots n_i - 1$; $i = 1, 2$. Find the corresponding column vector of coefficients of $a_1^{j_1} a_0^{j_0} q(a_1 a_0) \text{ modulo } [p; W_1(a_1), W_0(a_0)]$, which is equal to Q_j the j th column of corresponding matrix Q .

Procedure 2

Given $q(a_1 a_0)$ find the corresponding column vector of coefficients of $q(a_1 a_0)$, denoted by q . The j th column of the matrix Q corresponding to $q(a_1 a_0)$ is

$$Q_j = [W_1^{j_1} \otimes W_0^{j_0}] \cdot q \quad Q_0 = q$$

Example 2.6.8

Consider the Example (2.6.5).

Let $q(a_1, a_0) = 1 + a_0 + a_1 a_0 \in P_2^2[a_1^2 + 1] \cdot \otimes^T P_2^2[a_0^2 + a_0 + 1]$

$$W_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad W_0 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}; \quad q = \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \end{bmatrix}$$

Here, we have $n_0 = 2$; $n_1 = 2$.

The mixed radix representation of 0,1,2,3 reduce to the binary representation.

0	<0 0>
1	<0 1>
2	<1 0>
3	<1 1>

Therefore, $q_0 =$ coefficient of $a_1^0 a_0^0 = 1$

$$q_1 = \quad '' \quad a_1^0 a_0^1 = 1$$

$$q_2 = \quad '' \quad a_1^1 a_0^0 = 0$$

$$q_3 = \quad '' \quad a_1^1 a_0^1 = 1, \quad a_i^0 = 1, \quad i = 0, 1.$$

Then, $q = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$

We find the column of Q by the two procedures.

Procedure 1

Q_0 = zeroth column = column vector of coefficients of

$$q(a_1, a_0), \text{ i.e. } q = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \triangleq Q_0$$

Q_1 = first column = column vector of coefficients of

$$\begin{aligned} a_1^0 a_0^1 \cdot q(a_1, a_0) &= 1 + a_1 + a_0 a_1 \pmod{2; a_1^2 + 1, a_0^2 + a_0 + 1} \\ &= \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \end{aligned}$$

Q_2 = second column = column vector of coefficients of

$$\begin{aligned} a_1^1 a_0^0 \cdot q(a_1, a_0) &= a_0 + a_1 + a_1 a_0 \pmod{2; a_1^2 + 1, a_0^2 + a_0 + 1} \\ &= \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \end{aligned}$$

Q_3 = third column = column vector of coefficients of

$$\begin{aligned} a_1^1 a_1^1 \cdot q(a_1, a_0) &= 1 + a_0 + a_1 \pmod{2; a_1^2 + 1, a_0^2 + a_0 + 1} \\ &= \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \end{aligned}$$

Procedure 2

$$Q_0 : \text{zeroth column is } q = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

$$Q_1 : \text{First column : } [W_1^0 \otimes W_0^1] q = [I_2 \otimes W_0^1] q$$

$$= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

$$Q_2 : \text{Second column : } [W_1^1 \otimes W_0^0] \cdot q = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$Q_3 : \text{Third column : } [W_1^1 \otimes W_0^1] \cdot q = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$Q = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

*

Foregoing results of this section are now extended for the case $r > 2$. Given tensor product residue class polynomial

$$\text{ring } \bigotimes_{i=0, \dots, r-1}^T \{P_p^{n_i}[W_i(a_i)]\} \text{ we find}$$

$$M_p^{n_j}[W_j] \simeq P_p^{n_j}[W_j(a_j)] \text{ degree of } W_j(a_j) \text{ is } n_j,$$

$$j = 0, 1, \dots, r-1.$$

$\sum_{j=0}^{r-1} n_j = n$. Then the tensor product ring of nxn matrices

$$\bigotimes_{i=0, \dots, r-1}^T \{M_p^{n_i}[W_i]\} \simeq \bigotimes_{i=0, \dots, r-1}^T \{P_p^{n_i}[W_i(a_i)]\}.$$

If $q_{i_{r-1} i_{r-2} \dots i_0} a_{r-1}^{i_{r-1}} a_{r-2}^{i_{r-2}}, \dots, a_1^{i_1} a_0^{i_0} \in \bigotimes_{i=0, \dots, r-1}^T \{P_p^{n_i}[W_i(a_i)]\}$

then the nxn matrix corresponding to this element is

$$q_{i_{r-1} i_{r-2} \dots i_1 i_0} (W_{r-1}^{i_{r-1}} \otimes W_{r-2}^{i_{r-2}} \otimes \dots \otimes W_1^{i_1} \otimes W_0^{i_0}). \text{ In}$$

general

$$q(a_{r-1}, \dots, a_1 a_0) = \sum_{i=\langle i_{r-1} \dots i_0 \rangle}^{n-1} q_{i_{r-1} i_{r-2} \dots i_1 i_0} a_{r-1}^{i_{r-1}} \dots a_1^{i_1} a_0^{i_0} \in \bigotimes_{i=0, \dots, r-1}^T \{P_p^{n_i}[W_i(a_i)]\}$$

the corresponding matrix is

$$Q = \sum_{i=\langle i_{r-1} \rangle}^{n-1} q_i (W_{r-1}^{i_{r-1}} \otimes W_{r-2}^{i_{r-2}} \dots \otimes W_1^{i_1} \otimes W_0^{i_0}).$$

where W_i is the companion matrix of $W_i(a_i)$, $i = 0, \dots, r-1$.

As in the case $r = 2$ here also it can be shown that the zeroth column of Q is

$$q = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{bmatrix}$$

where q_i is the coefficient of $a_{r-1}^{i_{r-1}} a_{r-2}^{i_{r-2}} \dots a_1^{i_1} a_0^{i_0}$ and $\langle i_{r-1} i_{r-2} \dots i_1 i_0 \rangle$ is the mixed radix representation of integer i with respect to mixed radices n_0, n_1, \dots, n_{r-1} . The j th column of Q can be found as follows.

Procedure 1

Column vector of coefficients of

$$a_{r-1}^{j_{r-1}} a_{r-2}^{j_{r-2}} \dots a_1^{j_1} a_0^{j_0} q_j(a_{r-1}, a_{r-2}, \dots, a_1, a_0) \text{ modulo } [p; W_{r-1}(a_{r-1}) \dots W_0(a_0)].$$

Procedure 2

$$(W_{r-1}^{j_{r-1}} \otimes W_{r-2}^{j_{r-2}} \otimes \dots \otimes W_1^{j_1} \otimes W_0^{j_0}) \cdot q \text{ where } \langle j_{r-1} j_{r-2} \dots j_1 j_0 \rangle$$

is the mixed radix representation of j with respect to mixed

radices n_0, n_1, \dots, n_{r-1} . That is, $j = \sum_{i=1}^{r-1} j_i \prod_{k=0}^{i-1} n_k + j_0$.

We now consider rings of n -tuples over $GF(p)$ isomorphic to residue class ring of polynomials of order p^n over $GF(p)$.

2.6.3 Rings $Z_p^n[W]$ of n-tuples over $GF(p)$ Isomorphic to $P_p^n[W(a)]$

We have seen in Section 2.1, that the set

$$\{a^0, a^1, a^2, \dots, a^{n-1}\} \quad (2.6.22)$$

Constitutes a basis of $P_p^n[W(a)]$. Any element of $P_p^n[W(a)]$ is a linear combination of (2.6.22) over $GF(p)$. With the correspondence

$$a^0 \rightleftharpoons \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \triangleq \underline{a}^0; \quad a^1 \rightleftharpoons \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \triangleq \underline{a}^1; \quad a^i \rightleftharpoons \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \triangleq \underline{a}^i \quad \begin{matrix} 1 \text{ at } i\text{th location.} \end{matrix}$$

$$a^{n-1} \rightleftharpoons \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \triangleq \underline{a}^{n-1}$$

Consider the set of n-tuples

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \dots, \quad \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

which constitutes a basis of set of all n-tuples of $GF(p)$. Any n-tuple over $GF(p)$ is then a linear combination of the above n-tuples.

$$\text{Let } q(a) = \sum_{i=0}^{n-1} q_i a^i \in P_p^n[W(a)]$$

The n-tuple corresponding to $q(a)$

$$q(a) = \sum_{i=0}^{n-1} q_i a^i \rightsquigarrow \sum_{i=0}^{n-1} q_i \underline{a}^i = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_i \\ \vdots \\ q_{n-1} \end{bmatrix} \triangleq \underline{q}$$

Hence there is a one to one correspondence between $q(a)$ and the n-tuple \underline{q} .

With the addition of two n-tuples defined as pointwise modulo p addition, the set of all n-tuples constitute an additive abelian group. We define the multiplication of two n-tuples as follows. The two n-tuples are expressed as polynomials. The polynomials are multiplied modulo $[p; W(a)]$. The coefficients of the resulting polynomial is written as an n-tuple. With these operations the set of all n-tuples $Z_p^n[W]$ over $GF(p)$ constitutes a commutative ring isomorphic to $P_p^n[W(a)]$. The inverse mapping

$$\text{is : } \underline{q} = \begin{bmatrix} q_0 \\ \vdots \\ q_{n-1} \end{bmatrix} \rightarrow q(a) = \sum_{i=0}^{n-1} q_i a^i .$$

We give below examples of rings of n-tuples over $GF(p)$ isomorphic to residue class rings of polynomials over $GF(p)$, and illustrate the procedure of multiplication.

Example 2.6.9

Consider $P_2^2[a^2+1]$. The elements of this ring are given in Example 2.6.1. The corresponding 2-tuples are

$$\left\{ \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\} . \text{ The addition in this ring is pointwise addition}$$

of 2-tuples modulo 2. Suppose we want to multiply two 2-tuples say $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$. We express them as polynomials a and

$(1+a)$, multiply them modulo $[2; (a^2+1)]$ which gives

$$a(1+a) = (a^2+a) = (1+a) \text{ modulo } [2; a^2+1] \neq \begin{bmatrix} 1 \\ 1 \end{bmatrix} .$$

$$\text{Therefore, } \begin{bmatrix} 0 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} .$$

Example 2.6.10

*

Consider $P_2^2[a^3+a^2+a+1]$. The elements of this ring are given in Example 2.6.2. The corresponding 3-tuples are

$$\left\{ \begin{array}{ccccccccc} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & , & 0 & , & 0 & , & 1 & , & 1 & , & 1 \end{array} \right\}$$

The addition in this ring is pointwise addition of 3-tuples modulo 2. Suppose we want to multiply two 3-tuples say

$$\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \quad ; \text{ we express these elements as polynomials}$$

$$\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \approx (1+a^2) ; \quad \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \approx a+a^2; \text{ multiply them } \cdot \text{ mod } [2, a^3+a^2+a+1] .$$

This gives $(1+a^2)(a+a^2) = a+a^2+a^3+a^4 = 0 \text{ mod}[2, a^3+a^2+a+1]$.

This corresponds to $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$.

The individual elements are not zero but the product is zero.

This implies that the elements under considerations are zero-divisors in the ring.

As another example consider the multiplication of $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

We express these elements as polynomials

$$\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \approx a ; \quad \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \approx (1+a+a^2); \text{ multiply them } \cdot$$

$\text{mod}[2; a^3+a^2+a+1]$. This gives $a+a^2+a^3 = 1 \text{ mod}[2; a^3+a^2+a+1]$

$$\approx \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} . \text{ Hence we have } \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Example 2.6.11

Consider $P_3^2[a^2-1]$ the elements of this ring are given in Example 2.6.3. The corresponding 2-tuples over $GF(3)$ are

$$\left\{ \begin{array}{cccccccccc} 0 & 1 & 2 & 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & , & 0 & , & 0 & , & 1 & , & 2 & , & 1 & , & 2 & , & 2 & , & 2 \end{array} \right\}$$

The addition in this ring is pointwise addition modulo 3. Multiplication of two 2-tuples say $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 2 \end{bmatrix}$ is carried out by expressing them as polynomials and multiplying them mod[3; a^2-1]

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix} \approx (2+a) \quad \text{and} \quad \begin{bmatrix} 2 \\ 2 \end{bmatrix} \approx 2+2a$$

$$(2+a)(2+2a) = 4+4a+2a+2a^2 = 1+2 = 0 \text{ mod}[3; a^2-1] \approx \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\text{Therefore, } \begin{bmatrix} 2 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

This implies that the two elements considered are zero divisors in the ring.

As another example consider the multiplication of $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$, $\begin{bmatrix} 1 \\ 2 \end{bmatrix} \approx (1+2a)$; $\begin{bmatrix} 2 \\ 1 \end{bmatrix} \approx (2+a)$. Their product is

$$(1+2a) \cdot (2+a) = 2+a+4a+2a^2 = (1+2a) \text{ modulo}[3; a^2-1] \approx \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

$$\text{Hence } \begin{bmatrix} 1 \\ 2 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

The multiplication in the ring Z_p^n of n -tuples given above can be viewed alternatively as an appropriate matrix vector multiplication over $GF(p)$. This point of view is similar to the one used in [8,12,13] and as we shall see in Chapter 3, is useful in the implementation of $Z_p^n[W]$ -LSS $\simeq P_p^n[W(a)]$ -LSS.

Let $W(a) = \omega_0 + \omega_1 a + \dots + \omega_{n-1} a^{n-1} + a^n$, $\omega_i \in GF(p)$, be the modulus polynomial of the ring $P_p^n[W(a)]$, and W its companion matrix.

$$\text{Let } q(a) = \sum_{i=0}^{n-1} q_i a^i \in P_p^n[W(a)] \quad (2.6.23)$$

$$q(a) \approx \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{bmatrix} \approx q \quad (2.6.24)$$

Consider the product $a \cdot q(a)$ modulo $[p; W(a)]$

we have,

$$aq(a) = q_0 a + q_1 a^2 + \dots + q_{n-2} a^{n-1} + q_{n-1} a^n.$$

But $a^n = -(\omega_0 + \omega_1 a + \dots + \omega_{n-1} a^{n-1}) \text{ modulo } [p; W(a)]$.

$$\begin{aligned} \text{Therefore, } aq(a) &= -q_{n-1}\omega_0 + (q_0 - q_{n-1}\omega_1)a + (q_1 - q_{n-1}\omega_2)a^2 + \dots \\ &\quad + (q_{n-2} - q_{n-1}\omega_{n-1})a^{n-1} \end{aligned} \quad (2.6.25)$$

Let q' denote the coefficients of $aq(a)$ modulo $W(a)$. Then

$$q^1 = \begin{bmatrix} -q_{n-1} \omega_0 \\ q_0 - q_{n-1} \omega_1 \\ \vdots \\ q_{n-2} - q_{n-1} \omega_{n-1} \end{bmatrix} \quad (2.6.26)$$

As seen in Subsection 2.6.1

$$W \cdot q = \begin{bmatrix} 0 & 0 & \dots & 0 & -\omega_0 \\ 1 & 0 & \dots & 0 & -\omega_1 \\ \vdots & & & & \\ 0 & 0 & 0 \dots & 1 & -\omega_{n-1} \end{bmatrix} \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{bmatrix} \quad (2.6.27)$$

$$= \begin{bmatrix} -q_{n-1} \omega_0 \\ q_0 - q_{n-1} \omega_1 \\ q_1 - q_{n-1} \omega_2 \\ \vdots \\ q_{n-2} - q_{n-1} \omega_{n-1} \end{bmatrix} = q^1 \quad (2.6.28)$$

Thus multiplication of $q(a)$ by a and reduction to modulo $W(a)$ can be achieved by the multiplication of matrix W and vector q . Hence $aq(a) \equiv Wq$. In general, we have

$$a^i q(a) \equiv W^i q$$

Suppose $y(a) = g(a) \cdot q(a)$

Then from the above discussion we see that

$$y = \begin{bmatrix} \sum_{i=0}^{n-1} g_i w^i \end{bmatrix} q \quad (2.6.29)$$

$$\text{i.e., } y = g(W^1) q = G q \quad (2.6.30)$$

Since the multiplication in $P_p^n[W(a)]$ is commutative

$$y(a) = g(a) \cdot q(a) = q(a) \cdot g(a)$$

$$\text{we have } y = g(W) q = q(W) g = G q = Q g \quad (2.6.31)$$

Thus we see that if $g(a), q(a) \in P_p^n[W(a)]$

$g(a) \neq g$ and $q(a) \neq q$. The multiplication of the n -tuples q and g in the commutative ring of n -tuples, isomorphic to $P_p^n[W(a)]$ can be regarded as multiplication of matrix G and vector q or alternatively of matrix Q and vector g . With these operations Z_p^n is a commutative ring isomorphic to $P_p^n[W(a)]$.

We note here that in the multiplication of q and g the corresponding matrices Q or G are the same as the matrices in the commutative ring of $n \times n$ matrices corresponding to ring elements $q(a)$ and $g(a)$ respectively. Given $q(a)$ and the modulus polynomial $W(a)$ over $GF(p)$, the procedure to construct Q is discussed in Subsection 2.6.1. It is shown that with $q = Q_0$ as the zeroth column of Q the j th column of Q is given by $w^j Q_0 = W Q_{j-1}$.

Examples 2.6.12 to 2.6.14 given below, illustrate the multiplication operation in Z_p^n .

Example 2.6.12

Consider the ring $P_2^2[a^2+1]$. The ring of 2×2 matrices M_2^2 and ring of 2-tuples Z_2^2 isomorphic to $P_2^2[a^2+1]$ are given in Examples 2.6.1 and 2.6.9 respectively.

Suppose $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $Z_2^2 \simeq P_2^2[a^2+1]$ are to be multiplied. We have $a \neq \begin{bmatrix} 0 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $(1+a) \neq \begin{bmatrix} 1 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$.

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \neq a(1+a) \neq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \neq (1+a).$$

Alternatively,

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \neq (1+a) \cdot a \neq \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \neq (1+a).$$

*

Example 2.6.13

Consider the ring $P_2^3[a^3+a^2+a+1]$. The ring M_2^3 of 3×3 matrices and ring Z_2^3 of 3-tuples isomorphic to $P_2^3[a^3+a^2+a+1]$ are given in Examples 2.6.2 and 2.6.10 respectively.

i) Suppose $\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$ in $Z_2^3 \simeq P_2^3[a^3+a^2+a+1]$ are to be multiplied. We have $\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \neq (1+a)^2 \neq \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$ and

$$\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \approx (a+a^2) \approx \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \approx (1+a^2)(a+a^2) \\ \approx \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \approx 0.$$

Alternatively,

$$\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \approx (a+a^2) \cdot (1+a^2) \approx \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \approx 0$$

where arithmetic is modulo 2.

ii) Suppose $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ in $\mathbb{Z}_2^3 \approx \mathbb{P}_2^3[a^3+a^2+a+1]$ are to be multiplied. We have

$$\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \approx a \approx \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}; \quad \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \approx (1+a+a^2) \approx \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$\text{and} \quad \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \approx \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \approx 1$$

$$\text{Alternatively,} \quad \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \approx \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \approx 1$$

where arithmetic is modulo 2.

*

Example 2.6.14

Consider the ring $P_3^2[a^2-1]$. The ring M_3^2 of 2×2 matrices and ring Z_3^2 of 2-tuples isomorphic to $P_3^2[a^2-1]$ are given in Examples 2.6.2 and 2.6.11 respectively.

i) Suppose $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 2 \end{bmatrix}$ in Z_3^2 are to be multiplied.

We have $\begin{bmatrix} 2 \\ 1 \end{bmatrix} \approx (2+a) \approx \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 2 \end{bmatrix} \approx (2+2a) \approx \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$.

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \end{bmatrix} \approx \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \approx 0. \text{ Alternatively,}$$

$$\begin{bmatrix} 2 \\ 2 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} \approx \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \approx 0 \text{ where arithmetic is}$$

modulo 3.

ii) Suppose $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ are to be multiplied.

We have $\begin{bmatrix} 1 \\ 2 \end{bmatrix} \approx (1+2a) \approx \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 1 \end{bmatrix} \approx (2+a) \approx \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} \approx \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \approx (1+2a).$$

Alternatively, $\begin{bmatrix} 2 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} \approx \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \approx (1+2a)$

where arithmetic is modulo 3.

*

When the ring Z_p^n of n -tuples is isomorphic to $P_p^n[a^n-1]$, the corresponding $n \times n$ matrices used in the multiplication of two n -tuples, are cyclic matrices.

We next consider ring of n-tuples isomorphic to

$$\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}.$$

2.6.4 Ring $\bigotimes^T \{Z_p^{n_i}[W_i]\}$ of n-tuples over GF(p) Isomorphic to

$$\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$$

We will see that this case is an extension of the case discussed in Subsection 2.6.3. The ring of n-tuples isomorphic to $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ will be shown to be a linear combination of a set of Kronecker products of n_i -tuples $i = 0, 1, \dots, r-1$, obtained in the single variable case discussed in Subsection 2.6.3. We first consider the case $r = 2$.

Consider the tensor product of two residue class polynomial rings $P_p^{n_1}[W_1(a_1)]$ and $P_p^{n_0}[W_0(a_0)]$ of order p^{n_1} and p^{n_0} respectively. As we have already discussed in Subsection 2.6.2, the tensor product $P_p^{n_1}[W_1(a_1)] \bigotimes^T P_p^{n_0}[W_0(a_0)]$ is a ring of order p^n where $n = n_1 n_0$. The elements of this ring are polynomials in two variables a_1 and a_0 and the ring elements of the form $a_1^{i_1} a_0^{i_0}$ with $0 \leq i_1 \leq (n_1-1)$, and $0 \leq i_0 \leq (n_0-1)$ are linearly independent and constitute a basis of the tensor product ring.

We show below that it is possible to obtain a ring of n-tuples over GF(p) which is isomorphic to $P_p^{n_1}[W_1(a_1)] \bigotimes^T P_p^{n_0}[W_0(a_0)]$ $P_p^{n_0}[W_0(a_0)]$.

We have seen in Subsection 2.6.3 that there is a one-to-one correspondence between the basis $\{a_1^0, a_1^1, \dots, a_1^{n_1-1}\}$ of

$P_p^{n_1}[W_1(a_1)]$ and the set of n_1 tuples $\{\underline{a}_1^0, \underline{a}_1^1, \underline{a}_1^i, \dots, \underline{a}_1^{n_1-1}\}$

$$\text{where } \underline{a}_1^{i_1} \approx \underline{a}_1^{i_1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}; \text{ 1 in the } i_1 \text{th position.}$$

Consider $\underline{a}_1^{i_1} \in P_p^{n_1}[W_1(a_1)]$, $\underline{a}_0^{i_0} \in P_p^{n_0}[W_0(a_0)]$ and

$$\underline{a}_1^{i_1} \underline{a}_0^{i_0} \in P_p^{n_1}[W_1(a_1)] \times P_p^{n_0}[W_0(a_0)].$$

We apply the correspondence between n_j -tuple and $\underline{a}_j^{i_j}$; $j=0,1,\dots$ in two stages. First we treat $\underline{a}_0^{i_0}$ as a fixed element.

$$\underline{a}_1^{i_1} \underline{a}_0^{i_0} \approx \underline{a}_1^{i_1} \underline{a}_0^{i_0} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \underline{a}_0^{i_0}; \text{ 1 in } i_1 \text{th position.}$$

$$= \begin{bmatrix} 0.\underline{a}_0^{i_0} \\ 0.\underline{a}_0^{i_0} \\ \vdots \\ 1.\underline{a}_0^{i_0} \\ \vdots \\ 0.\underline{a}_0^{i_0} \end{bmatrix}; \text{ 1.}\underline{a}_0^{i_0} \text{ in } i_1 \text{th position.}$$

Now applying the correspondence between n_0 tuple and $a_0^{i_0}$ we have each 0 replaced by n_0 zeros and $a_0^{i_0}$ replaced by an n_0 -tuple with 1 in the i_0 th location

$$a_1^{i_1} a_0^{i_0} \rightsquigarrow \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Thus in the vector corresponding to $a_1^{i_1} a_0^{i_0}$, 1 appears in the $(n_0 i_1 + i_0)$ th location.

We see that $a_1^{i_1} a_0^{i_0}$ corresponds to the n -tuple which is the Kronecker product of n_1 -tuple corresponding to $a_1^{i_1}$ and n_0 -tuple corresponding to $a_0^{i_0}$.

That is,

$$a_1^{i_1} a_0^{i_0} \rightsquigarrow \underline{a_1^{i_1}} \otimes \underline{a_0^{i_0}}$$

Consider the set of n -tuples; where $n = n_1 n_0$,

$$\begin{array}{l} \{a_1^0 \otimes a_0^0, a_1^0 \otimes a_0^1, \dots, a_1^0 \otimes a_0^{n_0-1} \\ a_1^1 \otimes a_0^0, a_1^1 \otimes a_0^1, \dots, a_1^1 \otimes a_0^{n_0-1} \\ \vdots \\ a_1^{n_1-1} \otimes a_0^0, a_1^{n_1-1} \otimes a_0^1, \dots, a_1^{n_1-1} \otimes a_0^{n_0-1}\} \end{array}$$

The n -tuples in this set are linearly independent. The linear combinations of these n -tuples over $GF(p)$ constitute a tensor product of commutative ring of n_1 -tuples $Z_p^{n_1}[W_1]$ and n_0 -tuples $Z_p^{n_0}[W_0]$. The operations in this ring of n -tuples are (i) addition: pointwise addition modulo p and (ii) multiplication: express the two n -tuples as polynomials in $a_1 a_0$, multiply the polynomials modulo $[p; W_1(a_1), W_0(a_0)]$ and then write the coefficients of the resulting polynomial as n -tuple.

With the mapping $\phi: a_1^{i_1} a_0^{i_0} \in P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)]$

$$a_1^{i_1} \bar{x} a_0^{i_0} \in Z_p^{n_1}[W_1] \otimes^T Z_p^{n_0}[W_0],$$

$P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)] \cong Z_p^{n_1}[W_1] \otimes^T Z_p^{n_0}[W_0]$. This is proved in the theorem given below.

Theorem 2.6.6

The mapping $\phi: a_1^{i_1} a_0^{i_0} \rightarrow a_1^{i_1} \bar{x} a_0^{i_0}$ as defined above is an isomorphism between $Z_p^{n_1}[W_1(a_1)] \otimes^T Z_p^{n_0}[W_0(a_0)]$ and $P_p^{n_1}[W_1(a_1)] \otimes^T P_p^{n_0}[W_0(a_0)]$.

Proof

$$\text{Let } q(a_1, a_0) = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} a_1^{i_1} a_0^{i_0} \in P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)].$$

Then,

$$\phi(q(a_1, a_0)) = q = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} a_1^{i_1} \otimes a_0^{i_0} \quad (2.6.32)$$

Since q is a linear combination of linearly independent n -tuples $q = 0$ implies that the coefficients $q_{i_1 i_0} = 0, \forall i_1, i_0$. Therefore, only 0 of $P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]$ is mapped to null matrix. This implies $\text{Ker } \phi = 0$. Hence ϕ is one-to-one. Since the order of the two rings are same and is equal to p^n , ϕ is an isomorphism.

The inverse mapping ϕ^{-1} is obtained as follows :

$$\phi^{-1}: q = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_i \\ \vdots \\ q_{n-1} \end{bmatrix} = \begin{bmatrix} q_{\langle 0,0 \rangle} \\ q_{\langle 0,1 \rangle} \\ \vdots \\ q_{\langle i_1, i_0 \rangle} \\ \vdots \\ q_{\langle n_1-1, n_0-1 \rangle} \end{bmatrix} \rightarrow \sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} q_{i_1 i_0} a_1^{i_1} a_0^{i_0}$$

Example 2.6.15

Consider $P_2^2[a_1^2+1] \overset{T}{\otimes} P_2^2[a_0^2+a_0+1]$. The elements of this ring are given in Example 2.6.5. Consider the multiplication of 4-tuples.

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

we have $\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \approx (1+a_0)$ and $\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \approx (1+a_1)$

$$(1+a_0)(1+a_1) = 1+a_0+a_1+a_0a_1 \approx \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Hence $\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$

Example 2.6.16

*

Consider $P_2^2[a_1^2+1] \overset{T}{\otimes} P_2^3[a_0^3+1]$. The elements of this ring are given in Example 2.6.5. Consider the multiplication of 6-tuples

$$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad \text{we have}$$

$$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \neq 1+a_0^2+a_1 \quad \text{and} \quad \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \neq 1+a_0+a_1+a_1a_0 \quad \text{and}$$

$$(1+a_0^2+a_1)(1+a_0+a_1+a_1) = 1+a_0^2+a_1+a_0^2a_1 \pmod{2; a_1^2+1, a_0^3+1}$$

$$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

*

In the ring of n -tuples over $\text{GF}(p)$ isomorphic to $\bigotimes_{i=1}^n \mathbb{P}_p^i[W_i(a_i)]$ the multiplication operation can be viewed alternatively as an appropriate matrix and vector multiplication. This point of view is useful in the implementation of LSS over $\text{GF}(p)$ isomorphic to LSS over residue class ring of polynomials over $\text{GF}(p)$. We consider this next, for the case $r = 2$.

Consider $P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]$. Let $W_i(a_i)$ be of degree n_i , $i = 0, 1$. An element $q(a_0, a_1) \in P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]$ is of the form

$$\begin{aligned} q(a_0, a_1) = & q_0 + q_1 a_0 + q_2 a_0^2 + \dots + q_{n_0-1} a_0^{n_0-1} + \\ & q_{n_0} a_1 + q_{n_0+1} a_1 a_0 + q_{n_0+2} a_1 a_0^2 + \dots + q_{2n_0-1} a_1 a_0^{n_0-1} + \\ & \vdots \\ & + q_{(n_1-1)n_0} a_1^{n_1-1} + q_{(n_1-1)n_0+1} a_1^{n_1-1} a_0 + \dots \\ & q_{n_1 n_0-1} a_1^{n_1-1} a_0^{n_0-1} \end{aligned}$$

In vector notation we have

$$q = \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ \vdots \\ q_{n_1 n_0-1} \end{bmatrix}$$

where as indicated earlier, q_i the coefficient of $a_1^{i_1} a_0^{i_0}$ and $\langle i_1 i_0 \rangle$ is the mixed radix number system representation of i with respect to mixed radices n_0 and n_1 . That is,

$$i = n_0 i_1 + i_0.$$

Let us consider the product $a_1 a_0 \cdot q(a_0, a_1)$. We have

$$\begin{aligned}
a_1 a_0 \cdot q(a_0, a_1) &= q_0 a_1 a_0 + q_1 a_1 a_0^2 + q_2 a_1 a_0^3 + \dots q_{n_0-1} a_1 a_0^{n_0} \\
&\quad + q_{n_0} a_1^2 a_0 + q_{n_0+1} a_1^2 a_0^2 + q_{n_0+2} a_1^2 a_0^3 + \dots \\
&\quad q_{2n_0-1} a_1^2 a_0^{n_0} \\
&\quad \dots \quad \dots \\
&\quad \dots \quad \dots \\
&\quad \dots \quad \dots \\
&\quad + q_{(n_1-1)} a_1^{n_1} a_0 + q_{(n_1-1)n_0+1} a_1^{n_1} a_0^2 + \dots \\
&\quad q_{n_1 n_0-1} a_1^{n_1} a_0^{n_0}
\end{aligned} \tag{2.6.33}$$

The multiplication is modulo $w_i(a_i)$, $i = 0, 1$. Hence $a_i^{n_i}$ is expressed as a linear combination of $1, a_i, \dots, a_i^{n_i-1}$; using the relation ,

$$w_i(a_i) = w_{i0} + w_{i1} a_i + w_{i2} a_i^2 + \dots w_{in_i-1} a_i^{n_i-1} + a_i^{n_i} = 0 \quad i=0,1 \tag{2.6.34}$$

$$a_i^{n_i} = -(w_{i0} + w_{i1} a_i + w_{i2} a_i^2 + \dots w_{in_i-1} a_i^{n_i-1}) \quad i = 0,1 \tag{2.6.35}$$

Substituting (2.6.35) in (2.6.33) we get a new polynomial where the degree of a_i is less than n_i ; $i = 0, 1$.

In the polynomial $a_1 a_0 q(a_0, a_1) \bmod [p; w_1(a_1), w_0(a_0)]$
the constant term is $q_{n_1 n_0-1} w_{00} w_{10}$;
Coefficient of a_0 is $q_{n_1 n_0} w_{10} w_{01} - q_{(n_1-1) n_0} w_{10}$;
Coefficient of a_0^2 is $q_{n_1 n_0-1} w_{10} w_{02} - q_{(n_1-1) n_0+1} w_{10}$.

(2.6.36)

The multiplication by $a_1 a_0$ and reduction to modulo $w_1(a_1)$ and $w_0(a_0)$ can also be done by matrix multiplication.

Consider the companion matrix W_i of $w_i(a_i)$

$$W_i = \begin{bmatrix} 0 & 0 & 0 & \dots & -w_{i0} \\ 1 & 0 & 0 & \dots & -w_{i1} \\ 0 & 1 & 0 & \dots & -w_{i2} \\ 0 & 0 & 1 & \dots & -w_{i3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -w_{in_i-1} \end{bmatrix}$$

$i = 0, 1$.

Consider the vector-matrix product

$$(W_1 \otimes W_0)q = \begin{bmatrix} 0 & 0 & 0 & \dots & -w_{10} \\ 1 & 0 & 0 & \dots & -w_{11} \\ 0 & 1 & 0 & \dots & -w_{12} \\ 0 & 0 & 1 & \dots & -w_{13} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -w_{1n_1-1} \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 & 0 & \dots & -w_{00} \\ 1 & 0 & 0 & \dots & -w_{01} \\ 0 & 1 & 0 & \dots & -w_{02} \\ 0 & 0 & 1 & \dots & -w_{03} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -w_{0n_0-1} \end{bmatrix} q = q' \quad (2.6.37)$$

It is seen that

$$\begin{aligned} q'_0 &= q_{n_1 n_0 - 1} w_{10} w_{00} \\ q'_1 &= q_{n_1 n_0 - 1} w_{10} w_{01} - q_{(n_1 - 1) n_0} w_{10} \\ q'_2 &= q_{n_1 n_0 - 1} w_{10} w_{02} - q_{(n_1 - 1) n_0 + 1} w_{10} \end{aligned} \quad (2.6.38)$$

which are the coefficients of $a_1^0 a_0^0$, $a_1^0 a_0$, $a_1^0 a_0^2$ in $a_1 a_0 q(a_1, a_0)$ as given in Equation (2.6.36).

Thus we have $a_1 a_0 q(a_1, a_0) \bmod [p; W_1(a_1), W_0(a_0)] \neq (W_1 \otimes W_0) q$.

Likewise, it can be shown that

$$a_1^{j_1} a_0^{j_0} q(a_1, a_0) \neq W_1^{j_1} \otimes W_0^{j_0} q$$

The multiplication of n -tuples can hence be represented by matrix and vector product. The product of two n -tuples corresponding to $g(a_1, a_0)$ and $q(a_1, a_0)$ can then be represented by $G q$.

$$\text{where } G = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} g_{i_1 i_0} W_1^{i_1} \otimes W_0^{i_0} \quad (2.6.39)$$

Since the multiplication in $P_p^{n_1}[W_1(a_1)] \otimes P_p^{n_0}[W_0(a_0)]$ is commutative the product of $g(a_1, a_0)$ and $q(a_1, a_0)$ can also be represented by Qg

$$\text{where } Q = \sum_{i_1=0}^{n_1-1} \sum_{i_0=0}^{n_0-1} q_{i_1 i_0} W_1^{i_1} \otimes W_0^{i_0} \quad (2.6.40)$$

In general it can be analogously shown that for $r > 2$, the multiplication of two elements in the ring of n -tuples is multiplication of appropriate $n \times n$ matrix corresponding to one n -tuple and $n \times 1$ vector corresponding to the other n -tuple.

$$\text{If } q(a_{r-1}, a_{r-2}, \dots, a_1, a_0) = \sum_{i_{r-1}=0}^{n_{r-1}-1} \sum_{i_{r-2}=0}^{n_{r-2}-1} \dots \sum_{i_0=0}^{n_0-1} q_{i_{r-1}, i_{r-2}, \dots, i_0} a_{r-1}^{i_{r-1}} a_{r-2}^{i_{r-2}} \dots a_0^{i_0}$$

then the corresponding matrix is

$$Q = \sum_{i_{r-1}=0}^{n_{r-1}-1} \sum_{i_0=0}^{n_0-1} q_{i_{r-1} \dots i_0} W_{r-1}^{i_{r-1}} \otimes W_{r-2}^{i_{r-2}} \otimes \dots \otimes W_0^{i_0}$$

Given $q(a_{r-1} \dots a_1 a_0)$ the procedure of constructing Q is discussed in Subsection 2.6.2.

If $g(a_{r-1}, \dots, a_0)$ and $q(a_{r-1}, \dots, a_0) \in \bigotimes_{i=0}^{r-1} \{P_p^{n_i}[W_i(a_i)]\}^T$

With corresponding n -tuples g and q respectively, the multiplication of the n -tuples g and q can be regarded as multiplication of the matrix G and vector q or alternatively of matrix Q and vector g .

In the following examples we give the correspondence between elements of $\bigotimes_{i=0}^{r-1} \{P_p^{n_i}[W_i(a)]\}^T$ and $\bigotimes_{i=0}^{r-1} \{Z_p^{n_i}[W_i]\}^T$ and illustrate the multiplication in $\bigotimes_{i=0}^{r-1} \{Z_p^{n_i}[W_i]\}^T$.

Example 2.6.17

Consider $P_2^2[a_1^2+1] \otimes P_2^2[a_0^2+a_0+1]$ which is taken up in Examples 2.6.5 and 2.6.15. Consider the multiplication of

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \approx (1+a_0) \text{ and } \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \approx (1+a_1) \text{ as in Example 2.6.15.}$$

$$\text{We have } W_0 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad W_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$(1+a_0) \approx \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad (1+a_1) \approx \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

Hence

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \quad (1+a_0)(1+a_1) = 1+a_0+a_1+a_1a_0$$

alternatively,

$$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \quad (1+a_1)(1+a_0) = 1+a_0+a_1+a_1a_0$$

Example 2.6.18

Consider $P_2^2[a_1^2+1] \otimes^T P_2^3[a_0^3+1]$ which is taken up in Examples 2.6.6 and 2.6.16. Consider the multiplication of

$$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \approx (1+a_0^2+a_1) \quad \text{and} \quad \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \approx (1+a_0+a_1+a_1a_0)$$

We have $W_0 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$; $W_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and

$$(1+a_0^2+a_1) \approx [I_6+I_2 \otimes W_0^2+W_1 \otimes I_3] = \begin{bmatrix} 1 & 1 & 0 & | & 1 & 0 & 0 \\ 0 & 1 & 1 & | & 0 & 1 & 0 \\ 1 & 0 & 1 & | & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & | & 1 & 1 & 0 \\ 0 & 1 & 0 & | & 0 & 1 & 1 \\ 0 & 0 & 1 & | & 1 & 0 & 1 \end{bmatrix}$$

$$(1+a_0+a_1+a_1a_0) \approx [I_6+I_2 \otimes W_0+W_1 \otimes I_3+W_1 \otimes W_0] =$$

$$\begin{bmatrix} 1 & 0 & 1 & | & 1 & 0 & 1 \\ 1 & 1 & 0 & | & 1 & 1 & 0 \\ 0 & 1 & 1 & | & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & | & 1 & 0 & 1 \\ 1 & 1 & 0 & | & 1 & 1 & 0 \\ 0 & 1 & 1 & | & 0 & 1 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \approx \begin{bmatrix} 1 & 1 & 0 & | & 1 & 0 & 0 \\ 0 & 1 & 1 & | & 0 & 1 & 0 \\ 1 & 0 & 1 & | & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & | & 1 & 1 & 0 \\ 0 & 1 & 0 & | & 0 & 1 & 1 \\ 0 & 0 & 1 & | & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \approx$$

$$(1+a_0^2+a_1)(1+a_0+a_1+a_1a_0) = 1+a_0^2+a_1+a_1a_0^2$$

alternatively

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \approx \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

$$(1+a_0+a_1+a_1a_0)(1+a_0^2+a_1) = (1+a_0^2+a_1+a_1a_0^2)$$

The results of this section will be used in Section 3.5 in the implementation of LSS over GF(p).

*

CHAPTER 3

LINEAR SEQUENTIAL SYSTEMS OVER RESIDUE CLASS RINGS OF POLYNOMIALS OVER $GF(p)$

This chapter presents the state space description, implementation, input-output analysis, classification and decomposition of $P_p^n[W(a)]$ -LSS. LSS over the tensor product of residue class polynomial rings and other families of commutative rings isomorphic to $P_p^n[W(a)]$ -LSS are also considered. LSS over tensor product of residue class polynomial rings may be regarded as a generalisation of $P_p^n[W(a)]$ -LSS. Isomorphisms in $P_p^n[W(a)]$ -LSS lead to the notion of distinct classes of $P_p^n[W(a)]$ -LSS; the system over finite field $GF(p^n)$ constitute one of these distinct classes. Finally, implementation of $P_p^n[W(a)]$ -LSS in terms of isomorphic LSS over the ring of n -tuples over $GF(p)$ are given.

Section 3.1 gives the description of $P_p^n[W(a)]$ -LSS in terms of the state and output equations. The implementation of $P_p^n[W(a)]$ -LSS in terms of addition and multiplication operations in $P_p^n[W(a)]$ is considered in general. This is followed by serial implementation of $P_p^n[W(a)]$ -LSS in which

the addition and multiplication operations in $P_p^n[W(a)]$ are implemented serially in terms of $GF(p)$ arithmetic.

The input-output analysis of $P_p^n[W(a)]$ -LSS, taken up in Section 3.2, is of interest in applications such as sequence generators and sequence transformers for enciphering and encoding of data sequences to provide message privacy and error correction capability. Expressions for zero-input response and zero-state response have been derived. The response of nonsingular $P_p^n[W(a)]$ -LSS for periodic inputs and the periodicity properties of the resulting output are studied. It is shown that if the input is periodic with period J and period of A is T , then the output is also periodic whose period divides pJT . The autonomous response is studied in detail in Chapter 4.

In Section 3.3, we study classification and decomposition of $P_p^n[W(a)]$ -LSS. The classification of $P_p^n[W(a)]$ -LSS into nonsingular, singular or nilpotent $P_p^n[W(a)]$ -LSS is based on whether the characteristic matrix A is nonsingular, singular or nilpotent respectively. Conditions for A to be nilpotent and bound on the order of nilpotence of A and period of A are obtained using the results on the decomposition of rings discussed in Section 2.4. Determination of the period of nonsingular matrix A over finite field, local ring,

semisimple ring and semilocal ring are presented. The decomposition of $P_p^n[W(a)]$ leads to the notion of decomposition of LSS over semisimple or semilocal $P_p^n[W(a)]$ into LSS over orthogonal ideals in $P_p^n[W(a)]$ or over primary rings. Characteristic matrices A_1, A_2, \dots of component subsystems of a nonsingular $P_p^n[W(a)]$ -LSS are strictly periodic. Computation of period of A and study of autonomous response of $P_p^n[W(a)]$ -LSS can be carried out in terms of the subsystems of the decomposed $P_p^n[W(a)]$ -LSS.

LSS over other families of finite commutative rings are presented in Section 3.4. Towards this end we first consider LSS over tensor product of residue class polynomial rings and isomorphism between such systems and $P_p^n[W(a)]$ -LSS. Commutative rings $Z_p^n[W]$ and $M_p^n[W]$ isomorphic to $P_p^n[W(a)]$, and $\bigotimes^T \{Z_p^{n_i}[W_i]\}$ and $\bigotimes^T \{M_p^{n_i}[W_i]\}$ isomorphic to $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$, considered in Section 2.5 are utilised to obtain the LSS over these isomorphic rings. Isomorphism between $P_p^n[W(a)]$ -LSS and $Z_p^n[W]$ -LSS leads to the implementation of $P_p^n[W(a)]$ -LSS in terms of $Z_p^n[W]$ -LSS. $Z_p^n[W]$ -LSS of order K are a subclass of $GF(p)$ -LSS of order nK , which can process sequences of n -tuples over $GF(p)$ and whose analysis can be carried out in terms of $P_p^n[W(a)]$ -LSS. By means of examples, it is illustrated that for the above class of $GF(p)$ -LSS,

the computation of period of A is more compact and straightforward if carried out over $P_p^n[W(a)]$. Implementation of $\bigotimes_p^I \{Z_p^{n_i}[w_i]\}$ -LSS is also given. For the specific case of LSS over residue class polynomial rings with modulus polynomial (a^n-1) , the corresponding $Z_p^n[W]$ -LSS has an additional advantage that serial implementation of multiplication with serial output can be obtained, using cyclic shift registers and modulo p adders and scalars.

Isomorphisms in $P_p^n[W(a)]$ -LSS are studied in Section 3.6. In Section 2.3 we have seen that in contrast to finite fields, residue class polynomial rings of the same order need not be isomorphic to each other. Isomorphic residue class polynomial rings of a given order are said to belong to a class and the LSS defined over polynomial rings from such a class are said to constitute a distinct class of $P_p^n[W(a)]$ -LSS. Such a notion does not exist in the case of $GF(p^n)$ -LSS. In fact $GF(p^n)$ -LSS constitute a specific distinct class of $P_p^n[W(a)]$ -LSS. The number of distinct classes of $P_p^n[W(a)]$ -LSS for any specified order of $P_p^n[W(a)]$ are straight-away given by the number of nonisomorphic residue class rings of polynomials of the specified order as already given in Section 2.5.

3.1 STATE SPACE DESCRIPTION OF LSS OVER RESIDUE CLASS RINGS $P_p^n[W(a)]$ OF POLYNOMIALS OVER $GF(p)$:

Consider an m input, j output linear sequential system of order K over $P_p^n[W(a)]$. The elements of inputs, output and state sequences consist of m -tuples, j -tuples and K -tuples over $P_p^n[W(a)]$. The system is described in terms of the state and output equations, which give respectively the state at instant $(N+1)$ and output at instant N , in terms of state and input at instant N . Given the initial state $x(o)$ and input sequence $u(o), u(1), \dots$ the state and output sequences are obtained respectively from the state equations

$$\begin{bmatrix} x_o(N+1) \\ \vdots \\ x_{K-1}(N+1) \end{bmatrix} = \begin{bmatrix} a_{o,o} & \dots & a_{o,K-1} \\ \vdots & & \vdots \\ a_{K-1,o} & \dots & a_{K-1,K-1} \end{bmatrix} \begin{bmatrix} x_o(N) \\ \vdots \\ x_{K-1}(N) \end{bmatrix} \\
 + \begin{bmatrix} b_{o,o} & \dots & b_{o,m-1} \\ \vdots & & \vdots \\ b_{K-1,o} & \dots & b_{K-1,m-1} \end{bmatrix} \begin{bmatrix} u_o(N) \\ \vdots \\ u_{m-1}(N) \end{bmatrix} \quad (3.1.1)$$

and the output equation

$$\begin{bmatrix} y_0(N) \\ \vdots \\ y_{j-1}(N) \end{bmatrix} = \begin{bmatrix} c_{0,0} & \dots & c_{0,K-1} \\ \vdots & & \vdots \\ c_{j-1,0} & \dots & c_{j-1,K-1} \end{bmatrix} \begin{bmatrix} x_0(N) \\ \vdots \\ x_{K-1}(N) \end{bmatrix} \\
 + \begin{bmatrix} d_{0,0} & \dots & d_{0,m-1} \\ \vdots & & \vdots \\ d_{j-1,0} & \dots & d_{j-1,m-1} \end{bmatrix} \begin{bmatrix} u_0(N) \\ \vdots \\ u_{m-1}(N) \end{bmatrix} \quad (3.1.2)$$

Symbolically, Equations (3.1.1) and (3.1.2) may be written as,

$$x(N+1) = Ax(N) + Bu(N) \quad (3.1.3)$$

$$y(N+1) = Cx(N) + Du(N) \quad (3.1.4)$$

where,

$$x(N+1) = \begin{bmatrix} x_0(N+1) \\ \vdots \\ x_{K-1}(N+1) \end{bmatrix} \quad \text{is the state of the system at instant } (N+1)$$

$$u(N) = \begin{bmatrix} u_0(N) \\ \vdots \\ u_{m-1}(N) \end{bmatrix} \text{ is the input to the system at the instant } N$$

$$y(N) = \begin{bmatrix} y_0(N) \\ \vdots \\ y_{j-1}(N) \end{bmatrix} \text{ is the output from the system at instant } N$$

and matrices,

$$A = \begin{bmatrix} a_{0,0} & \cdots & a_{0,K-1} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ a_{K-1,0} & \cdots & a_{K-1,K-1} \end{bmatrix}; \quad B = \begin{bmatrix} b_{0,0} & \cdots & b_{0,m-1} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ b_{K-1,0} & \cdots & b_{K-1,m-1} \end{bmatrix}$$

$$C = \begin{bmatrix} c_{0,0} & \cdots & c_{0,K-1} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ c_{j-1,0} & \cdots & c_{j-1,K-1} \end{bmatrix} \text{ and } D = \begin{bmatrix} d_{0,0} & \cdots & d_{0,m-1} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ d_{j-1,0} & \cdots & d_{j-1,m-1} \end{bmatrix}$$

are called the characterising matrices of the system; A is specifically called the characteristic matrix and K , the size of A is called the order of the system.

$x(N)$ is called the present state and $x(N+1)$ is called the next state of the system.

Sometimes Equations (3.1.1) and (3.1.2) are also written as

$$x' = Ax + Bu \quad (3.1.5)$$

$$y = Cx + Du \quad (3.1.6)$$

where x is the present state and x' the next state of the system. u is the input to the system and y is the output from the system.

The sets of inputs, outputs and states constitute free modules over $P_p^n[W(a)]$, of rank m , j and K respectively. When $W(a)$ is irreducible over $GF(p)$, $P_p^n[W(a)]$ becomes $GF(p^n)$; the elements of input, output and state sequences are respectively, m -tuples, j -tuples and K -tuples over $GF(p^n)$, which constitute vector spaces of dimension m , j and K respectively.

Example 3.1.1:

Consider a second order LSS over $P_2^2[a^2+1] = \{0, 1, a, 1+a\}$ described by the equations,

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1+a & a \\ 1 & a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a \\ 1 \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 0 \\ a \end{bmatrix} u$$

where $x_0, x_1, y_0, y_1, u \in P_2^2[a^2+1]$. Here the characterising matrices are

$$A = \begin{bmatrix} 1+a & a \\ 1 & a \end{bmatrix} ; \quad B = \begin{bmatrix} a \\ 1 \end{bmatrix} ; \quad C = \begin{bmatrix} 1 & a \\ 1 & 0 \end{bmatrix} ; \quad \text{and } D = \begin{bmatrix} 0 \\ a \end{bmatrix} .$$

Sets of inputs outputs and states are free modules of rank, one, two and two respectively.

3.1.1 Implementation of $P_p^n[W(a)]$ -LSS:

Referring to Equation (3.1.1), we see that elements of state $x(N+1)$ are computed in terms of the elements of the state $x(N)$ and input $u(N)$ at instant N . Likewise from (3.1.2) we see that the elements of $y(N)$ at instant N are computed in terms of $x(N)$ and $u(N)$. These computations require subsystems which perform addition and multiplication operations in a residue class polynomial ring and also memory elements which store elements of state $x(N)$. Schematic representation of $P_p^n[W(a)]$ -LSS described by Equations (3.1.1) and (3.1.2) will be as shown in Figure 3.1.1.

$P_p^n[W(a)]$ -LSS can thus be implemented by a network of basic components called adders, scalars, and memory elements.

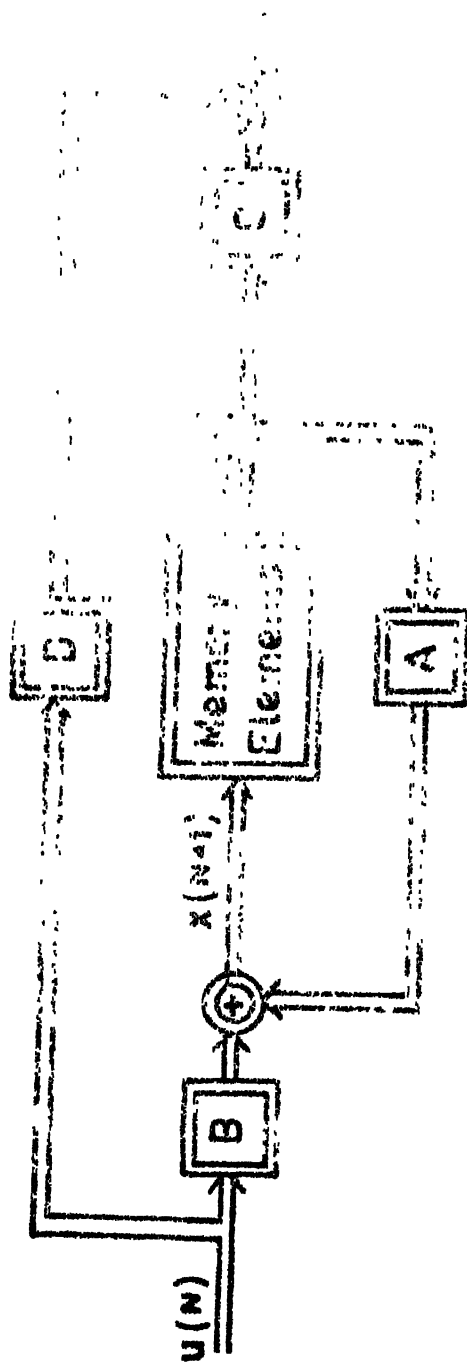


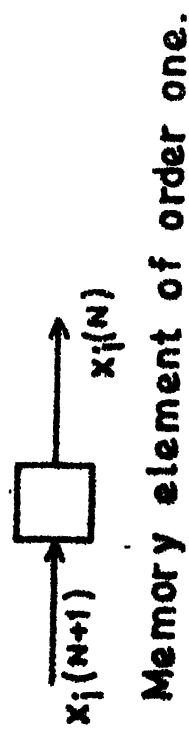
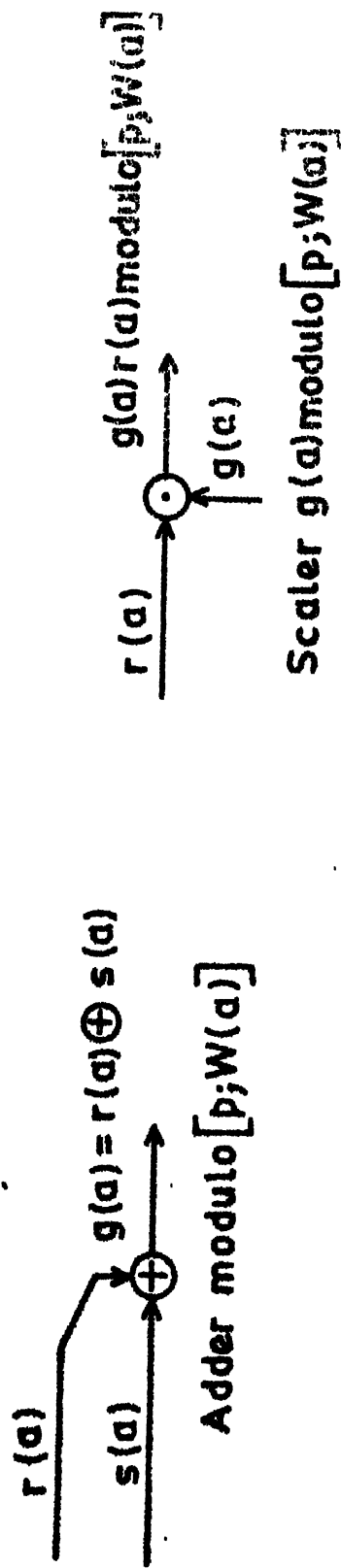
Fig.3.1.1 Schematic diagram of a system (USSR)

Adders perform the addition of two or more elements $\in P_p^n[W(a)]$. For the inputs say $r(a)$ and $s(a) \in P_p^n[W(a)]$ the output is

$$q(a) = r(a) + s(a) \in P_p^n[W(a)],$$

the addition is performed modulo $[p; W(a)]$. Scalers perform multiplication by a fixed element $g(a) \in P_p^n[W(a)]$. This is a single input single output component. If input is $r(a)$, output is $g(a).r(a)$ modulo $[p; W(a)]$. Memory element is a single input single output component. If $x(N+1)$ is the input at the $(N+1)$ th instant, the output is $x(N)$. The symbols for the basic components described above are given in Figure 3.1.2.

Consider an m -input and j -output $P_p^n[W(a)]$ -LSS of order K , whose state and output equations are given by Equations (3.1.1) and (3.1.2) respectively. Input is m -tuple, output is j -tuple, state is a K -tuple, A is a $K \times K$, B is a $K \times m$, C is a $j \times K$ and D is a $j \times m$ matrix over $P_p^n[W(a)]$. The schematic diagram of this LSS using the basic components adders, scalars and memory elements is shown in Figure 3.1.3. In this diagram, input and output lines are represented by m and j lines respectively. The s th input line and r th output line are denoted by u_s and y_r respectively. Scalars a_{ij} , b_{ij} , c_{ij} , d_{ij} are over $P_p^n[W(a)]$. Each input/output component gives rise to a terminal and each



$x_i(n), r(a), s(a), g(a) \in P_p^n[W(a)]$

Fig.3.1.2 Basic Components of $P_p^n[W(a)]$ LSS

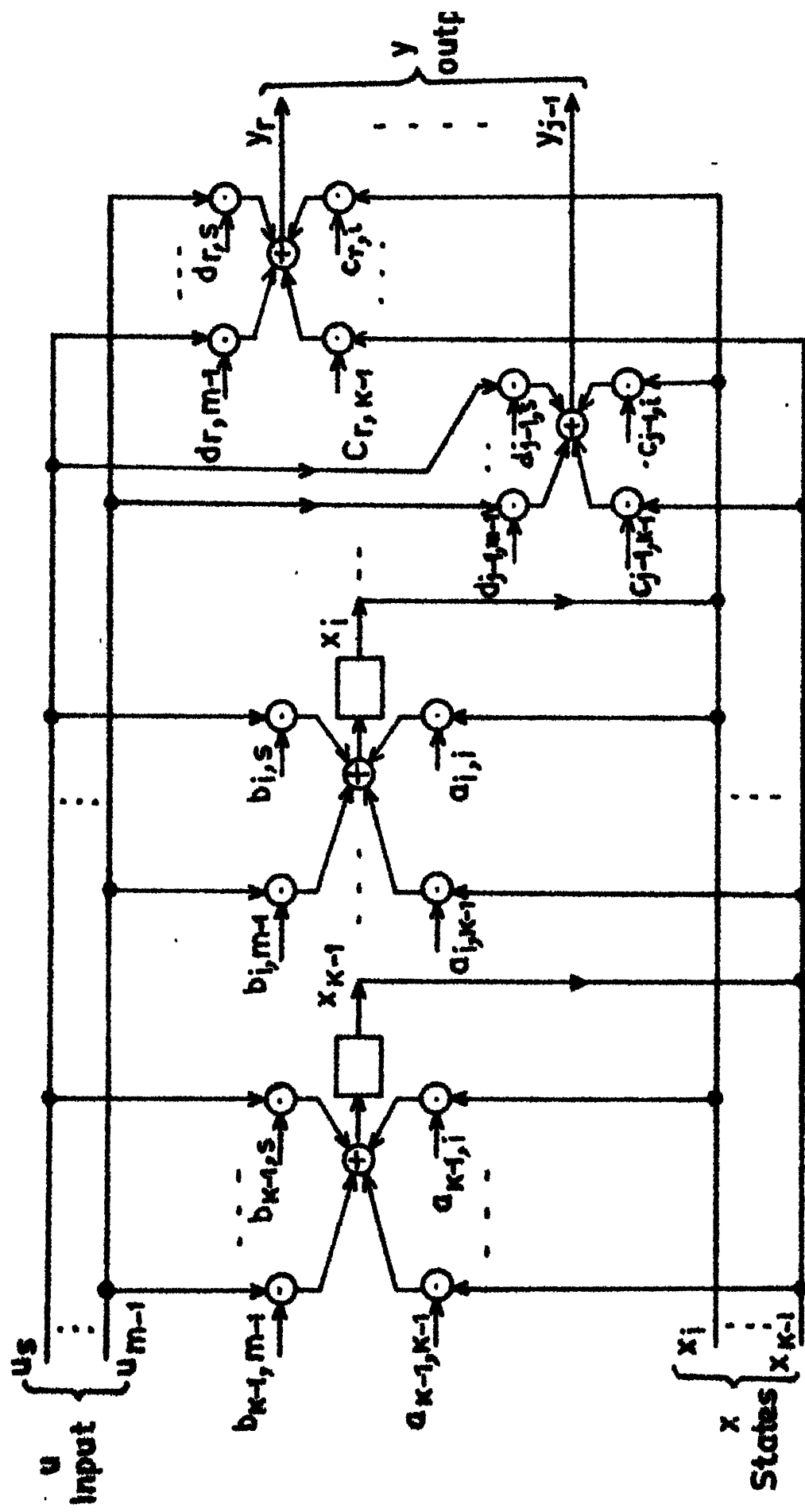


Fig.3.1.3 Implementation of LSS described by Equations
(3.1.1) and (3.1.2)

state component gives rise to a delay (memory) element.

The input and output of the i th memory element are denoted by x_i' and x_i respectively. Each input to memory element and each output terminal leaves from one adder. The inputs to the adder associated with the i th memory element $i = 0, 1, \dots, K-1$ are the outputs x_s each applied after multiplication by $a_{is} \in P_p^n[W(a)]$; $s = 0, 1, \dots, K-1$ and the inputs u_s each applied after multiplied by $b_{is} \in P_p^n[W(a)]$; $i = 0, 1, \dots, K-1$; $s = 0, 1, \dots, (m-1)$. The inputs to the adder associated with the output terminal y_r ; $r = 0, 1, \dots, (j-1)$ are the outputs x_s each applied after multiplication by $c_{rs} \in P_p^n[W(a)]$; $s = 0, 1, \dots, (K-1)$, and the inputs u_s each applied after multiplication by $d_{rs} \in P_p^n[W(a)]$, $r = 0, 1, \dots, (j-1)$ and $s = 0, 1, \dots, (m-1)$. The output elements y_i ; $i=0, 1, \dots, j-1$ are available from the output terminals. Two types of implementations of addition and multiplication are possible. In the first type the operations of addition and multiplications of elements from $P_p^n[W(a)]$ take place serially. As a consequence the operation is slow and the system needs two clocks, a faster clock for serial operation and a system clock which is n times slower than this. In the second type the operations of addition and multiplication of elements from $P_p^n[W(a)]$ take place in a parallel fashion in one period of the system clock.

Implementation of adder and scalars in $P_p^n[W(a)]$ -LSS:

Adders and scalars in $P_p^n[W(a)]$ can be implemented over $GF(p)$. Here we give serial implementation. Parallel implementation is discussed in Section 3.5.

Adders:

$$\text{Let } q(a) = \sum_{i=0}^{n-1} q_i a^i \text{ and } g(a) = \sum_{i=0}^{n-1} g_i a^i \in P_p^n[W(a)],$$

then the addition of $q(a)$ and $g(a)$ may be implemented with serial operation where $q(a) + g(a) = y(a) \text{ modulo } [p, W(a)]$

i) Serial operation: The coefficients q_i and g_i of $q(a)$ and $g(a)$ respectively are available in two registers. The corresponding coefficients q_i and g_i , $i=0,1,\dots,n-1$ are added modulo p in each clock period and stored in a third register. Only one 2-input modulo p adder is needed. The operation takes place in n clock periods. An additional clock which is n times slower acts as system clock. The scheme is shown in Figure 3.1.4.

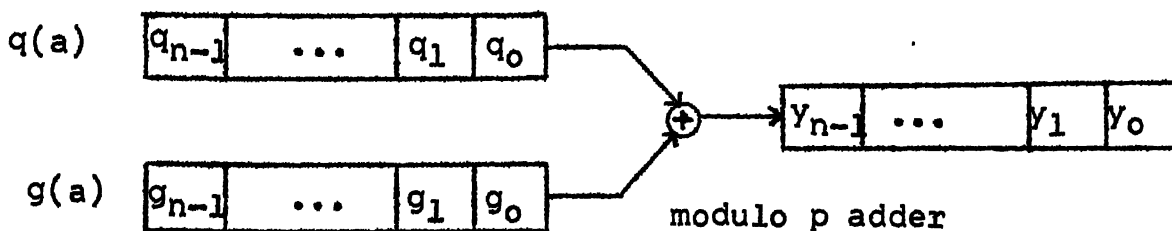


Fig. 3.1.4: Serial Implementation of Adder

Serial implementation of scaler $g(a) \in P_p^n[W(a)]$:

Let $g(a) = g_0 + g_1 a + \dots + g_{n-1} a^{n-1} \in P_p^n[W(a)]$:

and $w(a) = a^n + w_{n-1} a^{n-1} + \dots + w_1 a + w_0$; $g_i, w_i \in GF(p)$.

If the input to the scaler is $q(a) = \sum_{i=0}^{n-1} q_i a^i \in P_p^n[W(a)]$,

then the output of scaler $g(a)$ is

$$y(a) = q(a) \cdot g(a) \text{ modulo } [p; W(a)].$$

Thus the scaling is to be done in two steps.

- i) usual polynomial multiplication $q(a)g(a)$
- ii) finding the remainder $y(a)$ after dividing $q(a)g(a)$ by $W(a)$.

$$\text{Then } y(a) = q(a) g(a) \text{ modulo } [p; W(a)].$$

The operation of multiplication by $g(a)$ and division by $W(a)$ can be implemented in a single shift register circuit [12]. The scheme is given in Figure 3.1.5. The shift register is of n -stages. Each memory element stores element from $GF(p)$. Coefficients of polynomial $q(a) \in$

$P_p^n[W(a)]$ are fed in serially, with coefficient of highest degree term q_{n-1} , henceforth called highest degree symbol, entering first. After n clock pulses, coefficients of $y(a) = q(a) g(a) \text{ modulo } [p; W(a)]$ are stored in the memory elements. Since the operation is serial, two clocks are

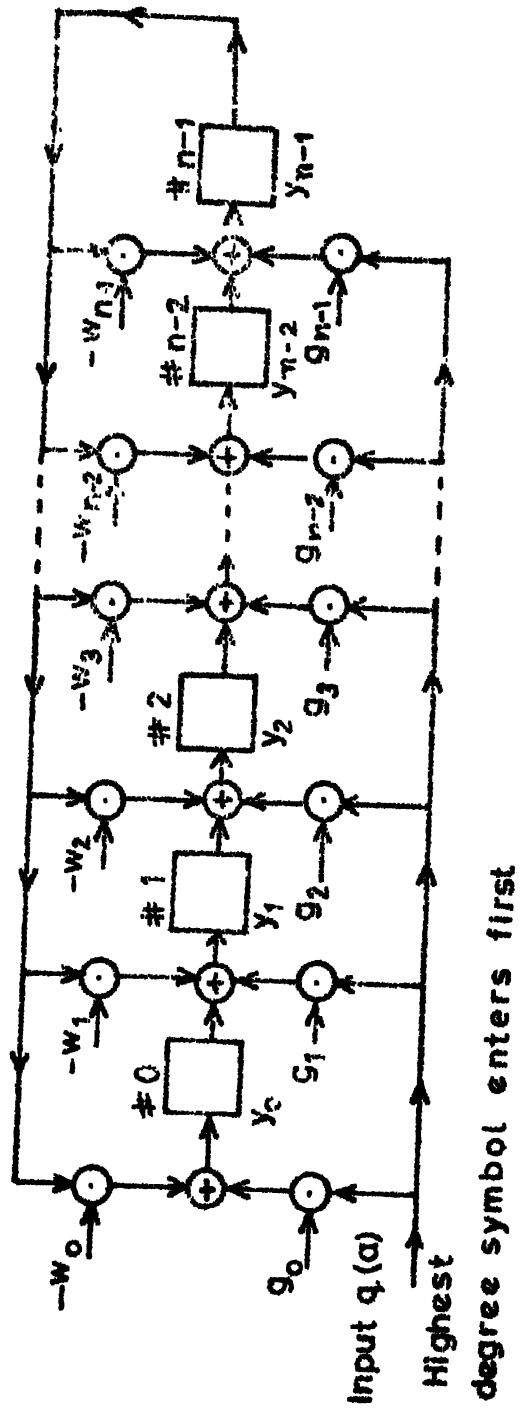


Fig.3.1.5 Serial Implementation of Scaler $g(a)$

required; a system clock, and another which operates n -times faster than the system clock, for serial operation.

The number of scalars over $GF(p)$ is at most $2n$.

The number of 2 or 3 input modulo p adders is at most n .

If $W(a) = a^n - 1$, the number of scalars over $GF(p)$ is at most n ; and 2-input adders modulo p are at most n .

Example 3.1.2:

Consider the scalar $(1+a^2) \in P_2^3 [a^3+a^2+a+1]$. The implementation over $GF(2)$ is given in Figure 3.1.6.

Consider the multiplication of $(1+a)$ by $(1+a^2)$. The input and contents of memory elements 0,1,2 are given below.

Instant	Input	Memory contents		
		0	1	2
0	-	0	0	0
1	0	0	0	0
2	1	1	0	1
3	1	0	0	0

The remainder is 0 since $(1+a^2)(1+a)$ modulo $[2, a^3+a^2+a+1] = 0$. Consider the multiplication of $(1+a^2)$ by $(1+a^2)$. The input and contents of memory elements 0,1,2 are given below.

Instant	Input	Memory contents		
		0	1	2
0	-	0	0	0
1	1	1	0	1
2	0	1	0	1
3	1	0	0	0

Consider the multiplication of $(1+a+a^2)$ by $(1+a^2)$

Instant	Input	Memory contents		
		0	1	2
0	-	0	0	0
1	1	1	0	1
2	1	0	0	0
3	1	1	0	1

$(1+a+a^2)(1+a^2)$ modulo $[2; a^3+a^2+a+1]$ is $(1+a^2)$.

Example 3.1.3:

Consider the scalar $(2+a) \in P_3^2[a^2+2a+1]$. The implementation over $GF(3)$ is given below in Figure 3.1.7.

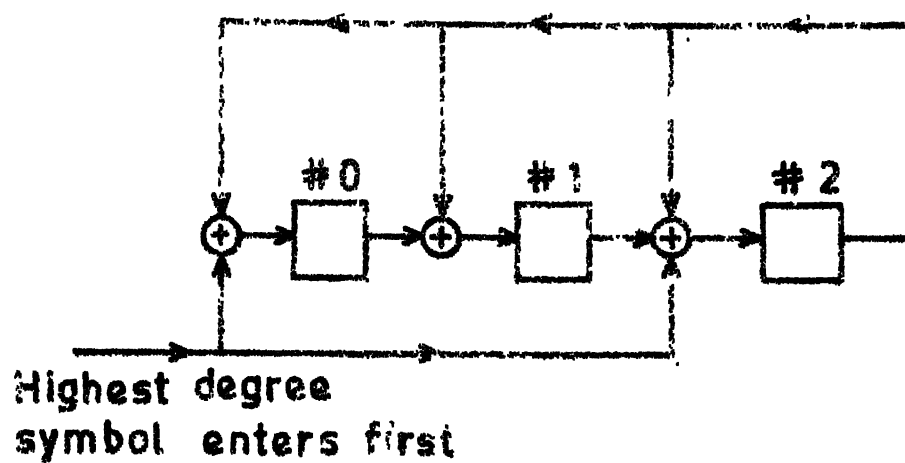


Fig.3.1.6 Scaler $(1+a^2)$ of Example 3.1.2

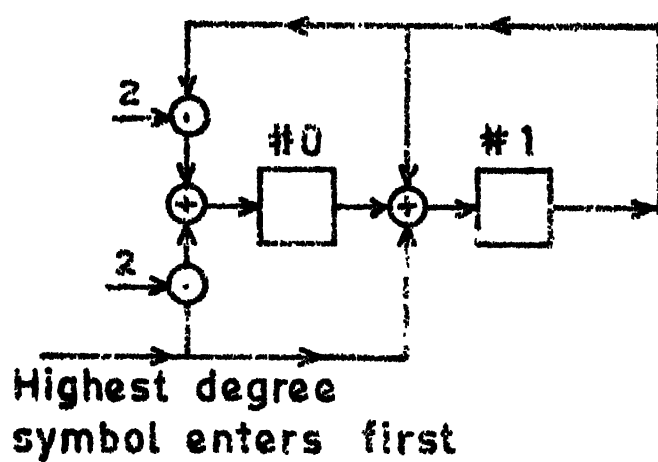


Fig.3.1.7 Scaler $(2+a)$ of Example 3.1.3

Consider the multiplication $(1+2a)(2+a)$ modulo $[3; a^2+2a+1]$.

Instant	Input	Memory contents	
		0	1
0	-	0	0
1	2	1	2
2	1	0	1

Hence $(1+2a)(2+a)$ modulo $[3; a^2+2a+1] = a$.

Consider the multiplication $(2+2a)(2+a)$ modulo $[3; a^2+2a+1]$.

Instant	Input	Memory contents	
		0	1
0	0	0	0
1	2	1	2
2	2	2	2

Hence $(2+2a)(2+a)$ modulo $[3; a^2+2a+1]$ is $(2+2a)$.

Example 3.1.4:

Consider the scalar $(1+a^2+a^3) \in P_2^4[a^4+1]$. The serial implementation is given in Figure 3.1.8.

Consider the multiplication $(a^3+a+1).(a^3+a^2+1)$ modulo $[2; a^4+1]$.

Instant	Input	Memory contents			
		0	1	2	3
0	-	0	0	0	0
1	1	1	0	1	1
2	0	1	1	0	1
3	1	0	1	0	1
4	1	0	0	0	1

Hence $(a^3+a+1).(a^3+a^2+1)$ modulo $[2; a^4+1]$ is a^3 .

Example 3.1.5:

Consider the scalar $(2+2a+a^2) \in P_3[a^3-1]$. The serial implementation is given in Figure 3.1.9.

Consider the multiplication $(1+2a+2a^2).(2+2a+a^2)$ modulo $[3; a^3-1]$.

Instant	Input	Memory contents		
		0	1	2
0	-	0	0	0
1	2	1	1	2
2	2	0	2	0
3	1	2	2	0

Hence $(1+2a+2a^2).(2+2a+a^2)$ modulo $[3; a^3-1]$ is $(2+2a)$.

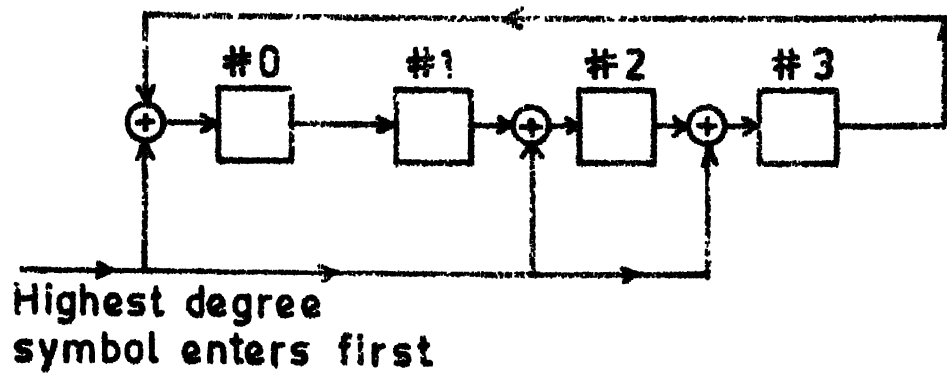


Fig.3.1.8 Scaler $(1 + a^2 + a^3)$ of Example 3.1.4

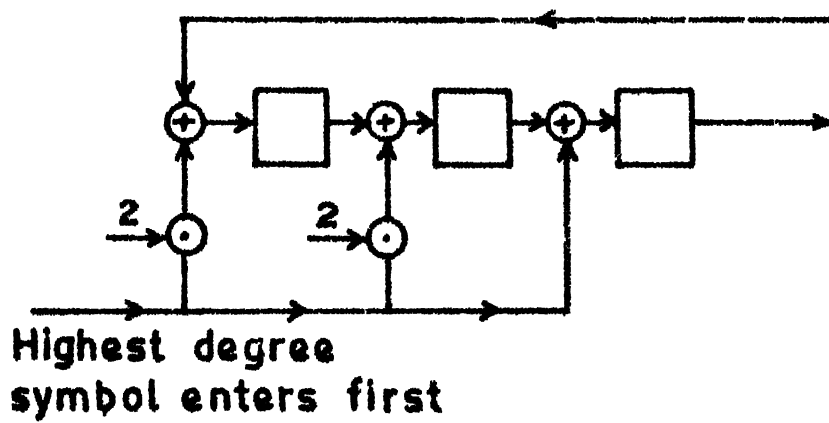


Fig.3.1.9 Scaler $(2 + 2a + a^2)$ of Example 3.1.5

The serial implementation of scaler discussed above is arranged such that if $q(a) \in P_p^n[W(a)]$ is to be multiplied by fixed polynomial $g(a)$, then the sequence of inputs is the sequence of coefficients $q_{n-1}, q_{n-2}, \dots, q_1, q_0$; in the descending order of powers of x . It is possible to obtain a serial implementation where the input sequence is $q_0, q_1, \dots, q_{n-2}, q_{n-1}$, in the ascending order of powers of x . In this case the scalars $-w_0, -w_1, -w_2, \dots, -w_{n-2}, -w_{n-1}$ and g_0, g_1, \dots, g_{n-1} are arranged in the reverse order. The operation remains the same. At the end of the operation, the coefficient y_i of $y(a)$ is stored in the $(n-1-i)$ th memory device; $i = 0, 1, 2, \dots, n-1$.

In Section 3.6 we give parallel implementation of scalars where the multiplication operation modulo $[p; W(a)]$ is performed in one clock cycle of the system, a second faster clock as in the case of serial implementation is not needed.

3.2 RESPONSE OF $P_p^n[W(a)]$ -LSS:

Given an initial state $x(0)$ and an input sequence $u(0), u(1), \dots$, the corresponding sequence $x(0), x(1), \dots$, of states is called state sequence and the sequence $y(0), y(1), \dots$ of outputs is called output sequence. State sequence and output sequence of $P_p^n[W(a)]$ -LSS can be computed recursively

from the state and output equations (3.1.1) and (3.1.2) of the system. These equations can also be solved to obtain directly the expressions for the state at (N+1)th instant and element of output sequence $y(N)$ at Nth instant, in terms of the initial state $x(o)$, input sequence and the characterising matrices. These expressions are given below.

$$x(N+1) = A^{N+1} x(o) + \sum_{i=0}^N A^{N-i} B u(i) \quad (3.2.1)$$

and

$$y(N) = CA^N x(o) + \sum_{i=0}^N H(N-i)u(i) \quad (3.2.2)$$

where,

$$\begin{aligned} H(N-i) &= D \text{ for } i = N \\ &= CA^{(N-i-1)} B \text{ for } i < N. \end{aligned}$$

The sequence $\{y(N)\}$ given by Equation (3.2.2) is called the total response. The response $\{y(N)\}$ obtained by setting $u(N) = 0$ for all $N \geq 0$ is called the autonomous response or zero input response $\{Y_{ZIR}(N)\}$ given by

$$Y_{ZIR}(N) = CA^N x(o) \quad (3.2.3)$$

Likewise, $x(N+1)$ with $u(N)=0$ for all $N \geq 0$ is called the autonomous state response given by $x(N+1) = A^{N+1} x(o)$. The response $\{Y_{ZSR}(N)\}$ obtained by setting $x(o) = 0$ in Equation (3.2.2) is called the zero state response.

$$y_{ZSR}(N) = \sum_{i=0}^N H(N-i)u(i) \quad (3.2.4)$$

We note here that the right hand side of Equation (3.2.4) represents the convolution operation.

Given any input sequence $\{u(N)\}$; $N = 0, 1, \dots$ and initial state $x(0)$, these two components can be found separately and then added up to get total response. At this stage we observe the following properties of responses.

i) If the elements of the input sequence belong to an ideal, then the elements of the output sequence also belong to the same ideal. If the elements of the matrices C and D belong to an ideal, the elements of the output sequence belong to the same ideal.

ii) In Equations (3.2.1) and (3.2.2), if the input sequence is periodic and A is periodic, then the state response and the total response are periodic. The zero state response given by Equation (3.2.4) is periodic, if A and $\{u\}$ are periodic and the autonomous response given by Equation (3.2.3) is periodic if A is periodic. The autonomous response of $P_p^n[W(a)]$ -LSS is taken up in Chapter 4. We will see that the autonomous response of a nonsingular $P_p^n[W(a)]$ -LSS is periodic, whose period divides the period of A . Thus in the study of response of $P_p^n[W(a)]$ -LSS the period of characteristic matrix A plays a prominent role.

3.2.1 Response to Periodic Inputs:

As we have already pointed out, although there is no satisfactory method for finding zero input and zero state responses simultaneously, for specific nonzero input sequences some gross properties of the total response may be obtained. Here we consider the system to be excited by a periodic sequence of period J . The result demonstrates the role played by the period of the characteristic matrix of LSS

The total response of a LSS, say L , is given by Equation (3.2.2) which is rewritten below.

$$y(N) = CA^N x(0) + \sum_{i=0}^N H(N-i)u(i)$$

where

$$\begin{aligned} H(N-i) &= D \text{ for } i = N \\ &= C A^{(N-i-1)} B \text{ for } i < N \end{aligned}$$

That is, $y(0) = Cx(0) + Du(0)$

and $y(N) = CA^N x(0) + \sum_{i=0}^{N-1} CA^{(N-i-1)} B u(i) + D u(N); N > 0.$

Theorem 3.2.1:

Let the input sequence $\{u(i)\} = \{u(0), u(1), \dots\}$ over a given ring, $P_p^n[W(a)]$ be periodic with period J . If the

characteristic matrix A is nonsingular with period T , i.e. $A^T = I$, then the output sequence,

$\{y(N)\} = (y(0), y(1), \dots)$ is periodic with period equal to a divisor of pJT .

Proof:

We have $y(0) = C x(0) + D u(0)$.

$$y(N) = C A^N x(0) + \sum_{i=0}^{N-1} C A^{N-i-1} B u(i) + D u(N) \quad N \geq 0$$

Consider $y(N+pJT)$.

$$\begin{aligned} y(N+pJT) &= C A^{N+pJT} x(0) + \sum_{i=0}^{N+pJT-1} C A^{N+pJT-i-1} B u(i) \\ &\quad + D u(N+pJT); \quad N \geq 0 \end{aligned}$$

But A is periodic with period T

Hence, $A^{pJT} = I$ and $A^{N+pJT} = A^N$,

and $u(i)$ is periodic with period J

Therefore $u(N+pJT) = u(N)$

$$\begin{aligned} y(N+pJT) &= C A^N x(0) + \sum_{i=0}^{N+pJT-1} C A^{N-i-1} B u(i) + D u(N) \\ &= C A^N x(0) + \sum_{i=0}^{N-1} C A^{N-i-1} B u(i) \\ &\quad + \sum_{i=N}^{N+pJT-1} C A^{N-i-1} B u(i) + D u(N) \dots \end{aligned} \quad (3.2.5)$$

Considering the third term in Equation (3.2.5) separately, we break this summation, into p summations as below.

$$\begin{aligned}
 \sum_{i=N}^{N+pJT-1} C A^{N-i-1} B u(i) &= \sum_{i=N}^{N+JT-1} C A^{N-i-1} B u(i) + \\
 \sum_{i=N+JT}^{N+2JT-1} C A^{N-i-1} B u(i) &+ \dots + \sum_{i=N+jJT}^{N+(j+1)JT-1} C A^{N-i-1} B u(i) \\
 + \dots + \sum_{i=N+(p-1)JT}^{N+pJT-1} C A^{N-i-1} B u(i) &\dots \quad (3.2.6)
 \end{aligned}$$

In each of the p summations in Equation (3.2.6), there are JT terms. Consider the first summation. Since the period of A is T and $\{u(i)\}$ is periodic with period J , we have,

$$\begin{aligned}
 \sum_{i=N}^{N+JT-1} C A^{N-i-1} B u(i) &= C [A^{-1}Bu(N) + A^{-2}Bu(N+1) \dots \\
 &+ A^{-JT} Bu(N+JT-1)] \quad (3.2.7) \\
 &= C [A^{T-1}Bu(N) + A^{T-2}Bu(N+1) + \dots + B u(N-1)]
 \end{aligned}$$

Likewise, the $(j+1)$ th summation,

$$\begin{aligned}
 \sum_{i=N+jJT}^{N+(j+1)JT-1} C A^{N-i-1} B u(i) &= C [A^{T-1} Bu(N) + A^{T-2} Bu(N+1) + \\
 &\dots + Bu(N-1)] \quad (3.2.8)
 \end{aligned}$$

Thus all the p summations on the right hand side in (3.2.6) are identical and the overall summation modulo p is identically equal to zero. Hence (3.2.5) becomes

$$\begin{aligned} y(N+pJT) &= C A^N x(0) + \sum_{i=0}^{N-1} C A^{N-i-1} B u(i) + D u(N) \\ &= y(N), \quad \forall N. \end{aligned} \quad (3.2.9)$$

Hence the output sequence is periodic. *

We next show that period of $\{y(i)\}$ divides pJT .

Let the period of the output sequence be k . By definition k is the least integer such that, $y(N+k) = y(N)$, $\forall N$.

Suppose k does not divide pJT , then we have,

$$pJT = kq+r \quad \text{where } 0 < r < L.$$

$$y(N) = y(N+pJT) = y(N+kq+r) = y(N+r), \quad \forall N$$

Hence period of $\{y(i)\}$ is $r < k$, which is a contradiction.

Hence $r = 0$ and $k|pJT$.

Remark 3.2.1:

The set of all inputs of period J constitutes a $P_p^n[W(a)]$ -module of finite rank J . The set of all total responses whose period divides pJT constitutes a $P_p^n[W(a)]$ -module of finite rank atmost pJT .

Example 3.2.1:

Consider a $p_2^2[a^2+1]$ -LSS with characterising matrices $A = [1]$, $B=[1]$; $C=[1]$ and $D=[0]$.

For the input, $(1 \ 0 \ a \ a \ 1 \ 0 \ a \ a \ \dots)$ the responses for the two cases, i) with initial state $(1+a)$ and ii) with initial state 1 are tabulated in Table 3.2.1.

Table 3.2.1: Input, state and output response of $p_2^2[a^2+1]$ -LSS of Example 3.2.1

Input	(i) Initial state (1+a)		(ii) Initial state 1	
	State	Output	State	Output
1	a	1+a	0	1
0	a	a	0	0
a	0	a	a	0
a	a	0	0	a
1	1+a	a	1	0
0	1+a	1+a	1	1
a	1	1+a	1+a	1
a	1+a	1	1	1+a
1	a	1+a	0	1
0	a	a	0	0
a	0	a	a	0
a	a	0	0	a
1	1+a	a	1	0
0	1+a	1+a	1	1
a	1	1+a	1+a	1
a	1+a	1	1	1+a
1	a	1+a	0	1
0	a	a	0	0

In this example $p=2$, $J=4$ and $T=1$

The output is periodic with period $pJT = 8$. If $C = [1+a]$ instead of $[1]$, the total response with initial state $(1+a)$ is $\{0, (1+a), (1+a), 0, (1+a), 0, 0, (1+a), 0, (1+a), (1+a), 0\}$ which is periodic with period equal to 8 but has elements only from the ideal $\{0, (1+a)\}$ in $P_2^2[a^2+1]$. Considering $Z_2^2[W]$ -LSS isomorphic to the given $P_2^2[a^2+1]$ -LSS, the corresponding input sequence of 2-tuples is

$$\begin{Bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & \dots \end{Bmatrix}. \text{ The output sequence}$$

for this input sequence with initial state $\begin{bmatrix} 1 \\ 1 \end{bmatrix} \neq (1+a)$ is

$$\begin{Bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & \dots \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & \dots \end{Bmatrix}$$

The output sequence with the initial state $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \neq 1$ is

$$\begin{Bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & \dots \end{Bmatrix}$$

The output with matrix $C = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \neq [1+a] = C$ and initial state $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is

$$\begin{Bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & \dots \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & \dots \end{Bmatrix}$$

Example 3.2.2:

Consider the 2nd order $P_2^2[a^2+1]$ -LSS which can be used as a sequence transformer given in Figure 3.2.1.

$A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$; period of A is 6.

Let the input be (0 a 0 a ...); a sequence of period 2.

Let the initial state be $[1 \ 0]^{\text{tr}}$. The inputs, states and outputs over $P_2^2[a^2+1]$ and the corresponding 2-tuples over $Z_2^2[W] \simeq P_2^2[a^2+1]$ are given in Table 3.2.2a. For the sake of convenience the 2-tuples are written as row 2-tuples. The period of the output is 6, which divides $2 \times 2 \times 6 = 24$.

Table 3.2.2a: Input, state and output of LSS of Example 3.2.2.

Instant	$P_2^2[a^2+1]$				$Z_2^2[W]$	
	Input	state		Output	Input	Output
		x_1	x_0			
0	0	0	1	a	00	01
1	a	0	0	0	01	00
2	0	0	0	0	00	00
3	a	a	0	1	01	10
4	0	1	a	1+a	00	11
5	a	1	1	0	01	00
6	0	0	1	a	00	01
7	a	0	0	0	01	00
8	0	0	0	0	00	00
9	a	a	0	1	01	10
10	0	1	a	1+a	00	11
11	a	1	1	0	01	00
12	0	0	1	a	00	01

Consider the input sequence $\{(1+a), 0, (1+a), 0 \dots\}$ of period 2. For the initial state $x_0 = 1$ and $x_1 = 0$, the input state and outputs over $P_2^2[a^2+1]$ and the corresponding 2-tuples over $Z_2^2[w] \simeq P_2^2[a^2+1]$ are given in Table 3.2.2b. The period of the output is 6 which divides 24.

Table 3.2.2b: Input, state and output of LSS of Example 3.2.2.

Instant	$P_2^2[a^2+1]$			$Z_2^2[w]$	
	Input	State $x_1 \quad x_0$		Output	Input Output
0	0	0	1		00
1	1+a	1	0	a	11 01
2	0	a	1	a	00 01
3	1+a	0	a	1+a	11 11
4	0	1	0	1	00 10
5	1+a	1	1	a	11 01
6	0	0	1	0	00 00
7	1+a	1	0	a	11 01
8	0	a	1	a	00 01
9	1+a	0	a	1+a	11 11
10	0	1	0	1	00 10
11	1+a	1	1	a	11 01
12	0	0	1	0	00 00

3.3 CLASSIFICATION AND DECOMPOSITION OF $P_p^n[W(a)]$ -LSS

We study the following topics.

- i) Classification of $P_p^n[W(a)]$ -LSS into nonsingular, singular and nilpotent systems based on the type of characteristic matrix A , namely nonsingular, singular or nilpotent respectively. Conditions for A to be nilpotent are obtained using the results on the decomposition of rings discussed in Section 2.4.
- ii) Computation of period of characteristic matrix A of nonsingular $P_p^n[W(a)]$ -LSS.
- iii) Decomposition of $P_p^n[W(a)]$ -LSS based on the decomposition of $P_p^n[W(a)]$. The properties of $P_p^n[W(a)]$ -LSS can then be studied in terms of the component subsystems over orthogonal ideal or primary ring.

3.3.1 Nonsingular, Singular and Nilpotent $P_p^n[W(a)]$ -LSS:

As we have seen in Section 3.2 the expression for $x(N+1)$ and $y(N)$ involve powers of A ; the characteristic matrix of $P_p^n[W(a)]$ -LSS. Thus the nature of response of $P_p^n[W(a)]$ -LSS is determined by the nature of its characteristic matrix A . Since the elements of A are from a residue class polynomial ring of finite order p^n , if we list the powers of A there will be repetition and the following cases may arise depending on the value of determinant of $A(|A|)$.

- i) $|A|$ is a unit in $P_p^n[W(a)]$, hence A and its powers are nonsingular [71,77] and there will be repetition in powers of A i.e., there exist least integers i and j , $i < j$, such that $A^i = A^j$

$$A^i = A^{i+(j-i)}$$

$$\text{Hence } A^i = A^{i+k(j-i)} = A^{i+kT} \quad k = 0, 1, \dots$$

since A^i is nonsingular this implies

$$I = A^{k(j-i)}$$

The least positive integer T for which $A^T = I$ is called the period of A . The sequence of its powers is periodic with period T . A is then called periodic with period T .

- ii) $|A|$ is either zero or zero divisor in $P_p^n[W(a)]$ and i and j , $i < j$, are the least integers such that $A^i = A^j$

$$\text{Hence } A^i = A^{i+k(j-i)} = A^{i+kT} \quad k = 0, 1, \dots$$

But for no integer m , $A^m = I$.

A is then singular [71,77] and sequence of its powers, $\{A^0 \triangleq I, A, A^2, \dots\}$ is ultimately periodic with period $(j-i) = T$.

A is then called ultimately periodic with period $(j-i) = T$.

iii) $|A|$ is either zero or zero divisor and if in addition,
 $A^i = 0$ for all $i \geq v$. Then A is called nilpotent
 matrix and v is called order (index) of nilpotence.

Example 3.3.1:

Consider $A = \begin{bmatrix} 1 & 0 \\ a & a \end{bmatrix}$ over $P_2^2[a^2 + 1]$

$$|A| = \begin{vmatrix} 1 & 0 \\ a & a \end{vmatrix} = a \text{ is a unit in } P_2^2[a^2+1].$$

Hence A is nonsingular

$$A^2 = \begin{bmatrix} 1 & 0 \\ a & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1+a & 1 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 1 & 0 \\ a & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1+a & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & a \end{bmatrix}$$

$$A^4 = \begin{bmatrix} 1 & 0 \\ a & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Hence, period of A is 4.

Example 3.3.2:

Consider $A = \begin{bmatrix} a & 0 \\ 1 & 0 \end{bmatrix}$ over $P_2^2[a^2+a+1] \cong GF(2^2)$

$|A| = 0$. Hence A is singular. Further A is ultimately
 periodic with period 3. We have,

$$A^2 = \begin{bmatrix} a & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a^2 & 0 \\ a & 0 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} a & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a^2 & 0 \\ a & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ a^2 & 0 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} a & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a^2 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 1 & 0 \end{bmatrix} = A$$

Example 3.3.3:

Consider $A = \begin{bmatrix} 1 & 0 \\ a & 1+a \end{bmatrix}$ over $P_2^2[a^2+1]$

$|A| = \begin{vmatrix} 1 & 0 \\ a & 1+a \end{vmatrix} = (1+a)$ is a zero divisor in $P_2^2[a^2+1]$.

A is therefore singular and

$$A^2 = \begin{bmatrix} 1 & 0 \\ 1 & 1+a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a & 1+a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ a & 0 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 1 & 0 \\ a & 0 \end{bmatrix} \text{ and } A^i = \begin{bmatrix} 1 & 0 \\ a & 0 \end{bmatrix} \text{ for all } i \geq 2.$$

Hence A is ultimately periodic with period 1.

Example 3.3.4:

Consider $A = \begin{bmatrix} (1+a^2) & (1+a) \\ a^2 & (1+a) \end{bmatrix}$ over $P_2^3[a^3+a^2+a+1]$

$|A| = (1+a)$ is a zero divisor in $P_2^3[a^3+a^2+a+1]$.

Hence A is singular.

$$A^2 = \begin{bmatrix} 1+a^2 & 1+1 \\ a^2 & 1+a \end{bmatrix} \begin{bmatrix} 1+a^2 & 1+a \\ a^2 & 1+a \end{bmatrix} = \begin{bmatrix} 1+a & 1+a^2 \\ a+a^2 & a+a^2 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 1+a^2 & 1+a \\ a^2 & 1+a \end{bmatrix} \begin{bmatrix} 1+a & 1+a^2 \\ a+a^2 & a+a^2 \end{bmatrix} = \begin{bmatrix} 1+a^2 & 1+a^2 \\ a+a^2 & 0 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} 1+a^2 & 0 \\ 0 & 1+a^2 \end{bmatrix}$$

$$A^5 = \begin{bmatrix} 0 & 0 \\ 1+a^2 & 0 \end{bmatrix}$$

$$A^6 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \underline{0}$$

Since $A^6 = \underline{0}$, A is nilpotent of order 6 over $P_2^3[a^3+a^2+a+1]$. *

If the characteristic polynomial $F(x) = |xI-A| = x^K - \sum_{i=1}^K a_i x^{K-i}$ of the matrix A over $P_p^n[W(a)]$ is known, the coefficients of the characteristic polynomial gives the information regarding the nature of the matrix A . If a_K is a unit in $P_p^n[W(a)]$, then A is nonsingular. If a_K is either zero or zero divisor in $P_p^n[W(a)]$, then A is singular. A bound on the order of nilpotence of a nilpotent matrix A is

obtained in terms of the order of nilpotence of the coefficients of $F(x)$. Towards this end we prove the following lemma.

Lemma 3.3.1:

An element $r(a)$ in a semilocal $P_p^n[W(a)]$; $\prod_{i=1}^v W_i^{h_i}(a)$, is nilpotent iff its internal and external direct sum components $r_i(a) \in J_i$ and $\tilde{r}_i(a) \in P_p^{h_i n_i}[W_i^{h_i}(a)]$ $i = 1, 2, \dots, v$ respectively, are nilpotent, where J_i is the orthogonal ideal generated by the orthogonal idempotent $e_i(a)$ in $P_p^n[W(a)]$ and $P_p^{h_i n_i}[W_i^{h_i}(a)]$ is the local ring isomorphic to J_i .

Proof:

Let $r(a)$ be a nilpotent element in $P_p^n[W(a)]$. Then there exists an integer j such that $(r(a))^j = 0$ modulo $[p; W(a)]$.

We have $P_p^n[W(a)] = J_1 + J_2 + \dots + J_v$ modulo $[p; W(a)]$, and $r(a) = r_1(a) + r_2(a) + \dots + r_v(a)$ modulo $[p; W(a)]$ where $r_i(a) \in J_i$

$$[r(a)]^j = [r_1(a) + r_2(a) + \dots + r_v(a)]^j$$

Since $r_i(a) \cdot r_k(a) = 0$ modulo $[p; W(a)]$, $i \neq k$ we have

$$[r(a)]^j = (r_1(a))^j + (r_2(a))^j + \dots + (r_v(a))^j = 0 \text{ modulo } [p; W(a)].$$

This implies $[r_i(a)]^j = 0$; $i = 1, 2, \dots, \nu$. Thus if $r(a)$ is nilpotent its internal direct sum components are also nilpotent.

On the other hand suppose

$$(r_i(a))^{j_i} = 0 \quad i = 1, 2, \dots, \nu$$

Let $\text{lcm}(j_1, j_2, \dots, j_\nu) = j$

$$\begin{aligned} &\text{then } (r_1(a))^j + (r_2(a))^j + \dots + (r_\nu(a))^j = \\ &(r_1(a) + r_2(a) + \dots + r_\nu(a))^j = 0 \text{ modulo } [p; W(a)]. \end{aligned}$$

$$\text{Hence } (r(a))^j = 0 \text{ modulo } [p; W(a)].$$

Thus $r(a)$ is nilpotent iff its internal direct sum components are nilpotent. Likewise the lemma can be proved for the case of external direct sum.

$$\text{Let } r(a) \neq [\tilde{r}_1(a), \tilde{r}_2(a), \dots, \tilde{r}_\nu(a)]$$

$$\text{where } \tilde{r}_i(a) = r(a) \text{ modulo } [p; W_i^{h_i n_i}(a)] \in P_p^{h_i n_i}[W_i^{h_i}(a)].$$

If $r(a)$ is nilpotent then there exists an integer j such that $[r(a)]^j = 0 \text{ modulo } [p; W(a)]$,

$$\text{Therefore } [r(a)]^j = 0 \neq [(\tilde{r}_1(a))^j, (\tilde{r}_2(a))^j, \dots, (\tilde{r}_\nu(a))^j] = [0 \dots 0]$$

$$\text{This implies } (\tilde{r}_i(a))^j = 0; r_i(a) \text{ is nilpotent in } P_p^{h_i n_i}[W_i^{h_i}(a)];$$

$i = 1, 2, \dots, \nu$. Thus the external direct sum components of $r_i(a)$ are nilpotent elements.

On the other hand let $\tilde{r}_i(a)$ be nilpotent with order of nilpotence j_i . Let $\text{lcm}(j_1, j_2, \dots, j_r) = j$ then $(\tilde{r}_i(a))^j = 0$ $i=1, 2, \dots, r$, and $(r(a))^j = [(\tilde{r}_1(a))^j, (\tilde{r}_2(a))^j, \dots, (\tilde{r}_r(a))^j] = [0, 0, \dots, 0]$.

Hence $(r(a))^j = 0$.

Thus $r(a)$ is nilpotent iff its external direct sum components are nilpotent. *

Remark 3.3.1:

The above result for the case of external direct sum can also be obtained by using the isomorphism between the internal direct sum and external direct sum components of $P_p^n[W(a)]$.

We now take up the condition for A to be nilpotent.

Theorem 3.3.1:

Let $F(x) = x^K - a_1 x^{K-1} - \dots - a_{K-1} x - a_K$, be the characteristic polynomial of A over semilocal $P_p^n[W(a)]$. Then A is nilpotent iff the coefficients a_1, a_2, \dots, a_K of $F(x)$ are either nilpotent or zero in $P_p^n[W(a)]$.

Proof:

A is nilpotent if some power of it is equal to the null matrix. Suppose a_i is nilpotent with order of nilpotence v_i , that is $a_i^{v_i} = 0$; if $a_i = 0$ we take $v_i = 1$, $i=1, 2, \dots, K$.

Let $v_m = \max \{v_1, v_2, \dots, v_K\} \leq p^j$

We have $x^K = \sum_{i=1}^K a_i x^{K-i}$ modulo $[p; F(x)]$

$$[x^K]p^j = \left[\sum_{i=1}^K a_i x^{K-i} \right] p^j = \sum_{i=1}^K a_i^{p^j} (x^{K-i})^{p^j}.$$

Since $a_i^{v_i} = 0$ and $p^j \geq v_i$

$$a_i^{p^j} = 0 \quad i = 1, 2, \dots, K$$

therefore $[x^K]p^j = 0$ modulo $[p; F(x)]$.

Since $F(x)$ is characteristic polynomial of A , by Cayley Hamilton theorem for matrices over commutative rings [71], $F(A) = \underline{0}$ and

$$A^K = \sum_{i=1}^K a_i A^{K-i} \text{ modulo } [p; F(A)], \text{ which leads to}$$

$$[A^K]p^j = \left[\sum_{i=1}^K a_i A^{K-i} \right] p^j = \sum_{i=1}^K a_i^{p^j} (A^{K-i})^{p^j} = \underline{0} \text{ modulo } [p; F(A)].$$

Therefore A is nilpotent, if coefficients of $F(x)$ are nilpotent. On the other hand suppose A is nilpotent, then there exists an integer v such that $A^v = \underline{0}$ modulo $[p; F(A)]$
or $x^v = 0$ modulo $[p; F(x)]$

Let $F_i(x) = F(x)$ modulo $[p; w_i^{h_i}(a)]$.

$$= x^K - a_{1,i} x^{K-1} - a_{2,i} x^{K-2} - \dots - a_{K,i}$$

where $a_{j,i} = a_i \text{ modulo } [p; W_i^{h_i}(a)]$; $j=1,2,\dots,K$ and $i=1,2,\dots,\nu$.
Hence $x^v = 0 \text{ modulo } [p; F_i(x)]$.

This implies that, there exists a polynomial $G_i(x) = g_{i,0} + g_{i,1}x + \dots g_{i,j-K}x^{j-K} + \dots$ such that $F_i(x) \cdot G_i(x) = x^v$, that is

$$x^v = (x^K - a_{1,i}x^{K-1} - a_{2,i}x^{K-2} \dots - a_{K,i})(g_{i,0} + g_{i,1}x + \dots g_{i,j-K}x^{j-K} + \dots)$$

Equating coefficients of like powers we have, coefficient of x^0

$$-a_{K,i} \cdot g_{i,0} = 0 \Rightarrow a_{K,i} \text{ is a zero divisor or zero} \quad (3.3.1)$$

coefficient of x ,

$$-a_{K,i} g_{i,1} - a_{K-1,i} g_{i,0} = 0$$

multiplying by $g_{i,0}$ and using the relation (3.3.1),

$$a_{K-1,i} g_{i,0}^2 = 0 \Rightarrow a_{K-1,i} \text{ is a zero divisor or zero} \quad (3.3.2)$$

coefficient of x^2 ,

$$-a_{K,i} g_{i,2} - a_{K-1,i} g_{i,1} - a_{K-2,i} g_{i,0} = 0$$

multiplying by $g_{i,0}^2$ and using the relation (3.3.1) and (3.3.2) we have

$$-a_{K-2,i} g_{i,0}^3 = 0 \Rightarrow a_{K-2,i} \text{ is a zero divisor or zero} \dots \quad (3.3.3)$$

Thus it can be shown that $a_{K-j,i} g_{i,0}^{j+1} = 0 \Rightarrow a_{K-j,i} = 0$

$0 \leq j \leq K-1$ is a zero divisor or zero.

$a_{j,i}; i=1,2,\dots,n$ are the external direct sum components of a_j . Since $a_{j,i} \in P_p^{h_i n_i} [W_i^{h_i}(a)]$ iff it is a zero divisor it is a multiple of $w_i^{h_i}(a)$. Hence $(a_{j,i})^{h_i} = 0$ modulo $[p; w_i^{h_i}(a)]$; $j=1,2,\dots,K; i=1,2,\dots,n$. Thus the external direct sum components of $a_j, j=1,2,\dots,K$ are nilpotent elements and from the result of Lemma 3.3.1, $a_j; j=1,2,\dots,K$ are nilpotent elements. Thus if A is nilpotent the coefficients of its characteristic polynomial are also nilpotent and thus the theorem is proved. *

Corollary 3.3.1:

If A is over semisimple $P_p^n[W(a)]$, then A is nilpotent iff its characteristic polynomial $F(x) = x^K$.

Proof:

In a semisimple ring there are no nilpotent elements. Hence from the result of Theorem 3.3.1 it follows that if A is nilpotent the coefficients a_1, a_2, \dots, a_K of characteristic polynomial of A , are zeros. Therefore $F(x) = x^K$.

On the other hand if $F(x) = x^K$ then $F(A) = A^K = \underline{0}$. Hence A is nilpotent.

Corollary 3.3.2:

If A is over finite field then A is nilpotent iff its characteristic polynomial $F(x) = x^K$.

Proof:

This is a special case of semisimple ring and the proof follows from Corollary 3.3.1. *

Having obtained the conditions for the characteristic matrix A to be nilpotent, we now take up bounds on the order of nilpotence of A . Towards this end we first prove the following Lemma.

Lemma 3.3.2: Let $F(x) = x^K - a_1 x^{K-1} - \dots - a_{K-1} x - a_K$, be the characteristic polynomial of $K \times K$ matrix A over $P_p^n[W(a)]$. If the elements a_i are nilpotent in $P_p^n[W(a)]$ and v_i is the least integer such that $a_i^{v_i} = 0$ for $i=1, 2, \dots, K$, then $A^{Kv'} = \underline{0}$ where $v' = \sum_{i=1}^K v_i - (K-1)$. $0 \in P_p^n[W(a)]$ is considered to be nilpotent element with order of nilpotence equal to 1.

Proof:

We prove the Lemma by induction. Suppose element $a_j \neq 0$, $a_i = 0$; $\forall i \neq j$ we then have $v' = v_j$, and $F(x) = x^K - a_j x^{K-j}$; by Cayley Hamilton theorem $F(A) = \underline{0}$. Hence $A^K = a_j A^{K-j}$, since $a_j^{v_j} = 0$ we have $A^{Kv'} = A^{Kv_j}$

$$= a_j^{v_j} (A^{K-j})^{v_j} = \underline{0}.$$

Suppose two elements a_i and a_j are nonzeros, then

$$v' = (v_i + v_j - 1) \text{ and}$$

$$x^K = a_i x^{K-i} + a_j x^{K-j}$$

$$A^K = a_i A^{K-i} + a_j A^{K-j}$$

$$A^{Kv'} = (a_i A^{K-i} + a_j A^{K-j})^{v'}$$

$$= (a_i A^{K-i})^{v'} + v' (a_i A^{K-i})^{(v'-1)} (a_j A^{K-j}) + \binom{v'}{2} (a_i A^{K-i})^2 (a_j A^{K-j})^2 + \dots + \binom{v'}{m} (a_i A^{K-i})^{v'-m} (a_j A^{K-j})^m + \dots$$

$$+ v' (a_i A^{K-i})^{v'-2} (a_j A^{K-j})^2 + \dots + \binom{v'}{m} (a_i A^{K-i})^{v'-m} (a_j A^{K-j})^m + \dots$$

$$+ v' (a_i A^{K-i}) (a_j A^{K-j})^{v'-1} + (a_j A^{K-j})^{v'} \dots \quad (3.3.4)$$

where

$$\binom{v'}{m} = \frac{v'!}{m!(v'-m)!}$$

$$\text{we have } v' = v_i + v_j - 1$$

$$v' - v_j = v_i - 1$$

$$\text{Thus if } m < v_j$$

$$(v' - m) > (v_i - 1)$$

$$(v' - m) \geq v_i$$

$$a_i^{(v'-m)} = 0$$

$$\text{and if } m \geq v_j, a_j^m = 0.$$

Hence all the terms on the right hand side of Equation (3.3.4) are $n \times n$ null matrices. Thus $A^{Kv'} = \underline{0}$.

Now we assume the lemma is true for $(K-1)$ nonzero elements, $a_1, a_2, \dots, a_{j-1}, a_{j+1}, \dots, a_K$; and show that it is true for K nonzero elements a_1, a_2, \dots, a_K

$$x^K = (a_1 x^{K-1} + \dots + a_{j-1} x^{K-j+1} + a_{j+1} x^{K-j-1} + \dots + a_K)$$

Let $v' = (v_1 + v_2 + \dots + v_{j-1} + v_{j+1} + \dots + v_K) - (K-2)$

Then by hypothesis $x^{Kv'} = (a_1 x^{K-1} + \dots + a_{j-1} x^{K-j+1} + a_{j+1} x^{K-j-1} + \dots + a_K)^{v'} = 0$

Assuming all the elements are nonzero, we have

$$x^K = [(a_1 x^{K-1} + \dots + a_{j-1} x^{K-j+1} + a_{j+1} x^{K-j-1} + \dots + a_K) + a_j x^{K-j}]$$

$$\begin{aligned} v' &= [(v_1 + v_2 + \dots + v_{j-1} + v_{j+1} + \dots + v_K) - (K-2)] + v_j - 1 \\ &= [(v_1 + v_2 + \dots + v_j + \dots + v_K) - (K-1)]. \end{aligned}$$

Treating the expression $\phi(x) = (a_1 x^{K-1} + a_{j-1} x^{K-j+1} + a_{j+1} x^{K-j-1} + \dots + a_K)$ as a single term we have,

$$\begin{aligned} A^{Kv'} &= [\phi(A) + a_j A^{K-j}]^{v'} \\ &= \phi(A)^{v'} + v'(\phi(A))^{v'-1} (a_j A^{K-j}) \\ &\quad + \binom{v'}{2} (\phi(A))^{v'-2} (a_j A^{K-j})^2 + \dots + \binom{v'}{m} (\phi(A))^{v'-m} \\ &\quad (a_j A^{K-j})^m + \dots + v'(\phi(A)) (a_j A^{K-j})^{v'-1} + (a_j A^{K-j})^{v'} \end{aligned}$$

(3.3.5)

We have $v' = v'' + v_j - 1$,

$$v' - v_j = (v'' - 1),$$

Therefore, if $m < v_j$; $(v' - m) > (v'' - 1)$ and $(\phi(A))^{v' - m} = \underline{0}$; by hypothesis and if $m \geq v_j$ $a_j^m = 0$, $j = 1, 2, \dots, K$.

Hence all the terms on the right hand side of Expression (3.3.5) are null matrices. Thus

$$A^{Kv'} = \underline{0}$$

The lemma is proved. *

Now we find the bound on the order of nilpotence of matrix A in terms of the order of nilpotence of the elements a_1, a_2, \dots, a_K .

Theorem 3.3.2:

Let A be a nilpotent matrix over $P_p^n[W(a)]$, with characteristic polynomial $F(x) = x^K - a_1 x^{K-1} - \dots - a_{K-1} x - a_K$. Let the elements $a_i \in P_p^n[W(a)]$, be nilpotent of order v_i ; $i = 1, 2, \dots, K$. Let $v_m = \max \{v_1, v_2, \dots, v_K\} \leq p^j$. Then A is nilpotent of order $\leq \min [Kp^j, K((\sum_{i=1}^K v_i) - (K-1))]$.

Proof:

From Theorem 3.3.1 . if $v_m = \max \{v_1, v_2, \dots, v_K\} \leq p^j$
then $A^{Kp^j} = \underline{0}$ and from Lemma 3.3.2

$$A^{K((\sum_{i=1}^K v_i) - (K-1))} = \underline{0}.$$

Therefore A is nilpotent of order $\leq \min[Kp^j, K((\sum_{i=1}^K v_i) - (K-1))]$.
Hence the proof. *

If the characteristic matrix A of $P_p^n[W(a)]$ -LSS is of the form

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_K & a_{K-1} & \dots & \dots & a_1 \end{bmatrix} \triangleq A_c, a_i \in P_p^n[W(a)]; i=1, 2, \dots, K,$$

then A_c is said to be in canonical form and the $P_p^n[W(a)]$ -LSS is called a canonical system.

For A_c over $P_p^n[W(a)]$ in canonical form the above results can be summarised as follows.

- i) A_c is nonsingular iff $|A_c| = a_K$ is a unit in $P_p^n[W(a)]$.
- ii) A_c is nilpotent iff a_i ; $i=1, 2, \dots, K$ are either zero or nilpotent.
- iii) If A_c is over a semisimple $P_p^n[W(a)]$ or a finite field, then it is nilpotent iff $a_i = 0$; $\forall i$
- iv) Order of nilpotence of A_c is $\leq \min [Kp^j, K((\sum_{i=1}^K v_i) - (K-1))]$, where v_i is the order of nilpotence of a_i , $i=1, 2, \dots, K$ and $p^j \geq \max \{v_1, v_2, \dots, v_K\}$.

Example 3.3.5:

Let $A_c = \begin{bmatrix} 0 & 1 \\ 1+a^2 & 1+a \end{bmatrix}$ be over $P_2^4[a^4+1]$; $a_1=(1+a)$ and

$a_2 = (1+a^2)$ are nilpotent elements with order of nilpotence 4 and 2 respectively in $P_2^4[a^4+1]$. A_c has the characteristic polynomial $F(x) = x^2 + (1+a)x + (1+a^2)$.

From Theorem 3.3.2 $K=2$, $p=2$; $j=2$, $v_1=4$, $v_2=2$.

Order of nilpotence of $A_c \leq \min [8, 10]$

Actual value is 5. That is 5 is the least integer such that $A_c^5 = 0$.

Example 3.3.6:

Considering the above example with a_1 and a_2 interchanged; that is, for

$$A_c = \begin{bmatrix} 0 & 1 \\ 1+a & 1+a^2 \end{bmatrix}$$

$$F(x) = x^2 + (1+a^2)x + (1+a)$$

The order of nilpotence of $A_c \leq \min [8, 10]$

Actual value is 8. *

3.3.2 Periodicity Properties of Characteristic Matrix A:

As we have seen in Section 3.2, the periodicity of output for a periodic input depends on the period of characteristic matrix A and as we shall see in Chapter 4, the

maximum possible period of autonomous response of a nonsingular $P_p^n[W(a)]$ -LSS, is equal to the period of the characteristic matrix A of the system. Thus period of A plays a prominent role in the response properties of $P_p^n[W(a)]$ -LSS. In this subsection we give procedures for computation of period of nonsingular matrix A . These are analogous to the determination of period of A over Z_m . The particular procedure used depends on the type of $P_p^n[W(a)]$ over which A is defined.

The following cases are considered.

- a) $P_p^n[W(a)]$ is a primary ring:
 - i) $W(a)$ irreducible over $GF(p)$; $P_p^n[W(a)]$ is a finite field
 - ii) $W(a)$ power of an irreducible polynomial over $GF(p)$; $P_p^n[W(a)]$ is a local ring.
- b) $P_p^n[W(a)]$ is isomorphic to direct sum of primary rings
 - iii) $W(a)$ product of irreducible polynomials over $GF(p)$; $P_p^n[W(a)]$ is a semisimple ring.
 - iv) $W(a)$ product of powers of irreducible polynomials over $GF(p)$; $P_p^n[W(a)]$ is a semilocal ring.

The computation of period T of A when it is over $GF(p)$ is discussed in [4,7,12,13,40]. The procedure can be extended to the case where A is over $GF(p^n)$.

1) $W(a)$ irreducible over $GF(p)$; A is over $GF(p^n)$:

Let degree of $W(a)$ be n , then $P_p^n[W(a)]$ becomes $GF(p^n)$; finite field of order p^n . Let α be a root of $W(a)$ in $GF(p^n)$. The set of all polynomials in α whose degree is less than n over $GF(p)$ are the elements in $GF(p^n)$ and if β is a primitive element, powers of β , that is $\beta, \beta^2, \dots, \beta^{p^n-1}$ are the nonzero elements in $GF(p^n)$. The characteristic matrix A is then over $GF(p^n)$. It is well known [4,12-14,40] that the period of a nonsingular matrix A over $GF(p^n)$ is determined by its minimal polynomial $m(x)$ (the least degree unique monic polynomial over $GF(p^n)$, such that $m(A)=\underline{0}$) [4,12-14,57]. A procedure for obtaining the minimal polynomial of A is outlined in Appendix D. If it is found that the constant term in $m(x)$ is zero the matrix A is singular. The following theorem relates the period of a nonsingular matrix A over $GF(p^n)$ and the period of its minimal polynomial [40].

Theorem 3.3.3:

The period of nonsingular matrix A over $GF(p^n)$ is equal to the period of its minimal polynomial $m(x)$.

Proof:

Let T be the period of $m(x)$. Then T is the least integer such that,

$$m(x) \mid (x^T - 1) \quad (3.3.6)$$

This implies $x^T = 1$ modulo $[p; m(x)]$

$m(x)$ is the minimal polynomial of A . Hence $m(A) = \underline{0}$ [40]

and $A^T = I$ modulo $[p; m(A)]$ *

The period of $m(x)$ can be determined by using the procedure [18] given in Appendix D, which involves computing the periods T_1, T_2, \dots, T_r of its factors $m_1^{h_1}(x), m_2^{h_2}(x), \dots, m_r^{h_r}(x)$, where $m_i(x); i=1, 2, \dots, r$ are irreducible over $GF(p^n)$ and computing the lcm of periods of T_1, T_2, \dots, T_r . Alternatively, the period of $m(x)$ can be obtained by finding the least integer T , such that, $x^T = 1$ modulo $[p; m(x)]$ [43]. Thus given $m(x)$ its period can be determined without performing the operation indicated in the expression (3.3.6).

Example 3.3.7:

Consider $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ over $GF(2)$; minimal polynomial $m(x)$ of A is $x^3 + x + 1$. Listing powers of x modulo 2 and $x^3 + x + 1$, we get, $x^3 = 1 + x$, $x^4 = x + x^2$, $x^5 = 1 + x + x^2$, $x^6 = 1 + x^2$, $x^7 = 1$.

Hence period of $m(x)$ and A are each equal to 7. *

Example 3.3.8:

Consider $A = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}$ over $GF(3)$, the minimal polynomial $m(x)$ of A (which is obtained as outlined in Appendix D) is $x^2 - x - 2 = (x^2 + 2x + 1)$ modulo 3. Listing power of x modulo 3

and (x^2+2x+1) , we get $x^2 = 2+x$, $x^3=2$, $x^4=2x$, $x^5=1+2x$ and $x^6=1$. Hence period of $m(x)$ and A are each equal to 6.

Example 3.3.9:

Let $A = \begin{bmatrix} 0 & \alpha \\ 1 & \alpha \end{bmatrix}$ over $GF(2^2)$, where $\alpha \in GF(2^2)$ and $\alpha^2+\alpha+1 = 0$. Minimal polynomial $m(x)$ of A over $GF(2^2)$ is $x^2+\alpha x+\alpha$. Listing powers of x modulo $[2; (\alpha^2+\alpha+1)]$ and $x^2+\alpha x+\alpha$, we get, $x^2 = \alpha+\alpha x$, $x^3=\alpha^2+x$, $x^4=\alpha+x$, $x^5=\alpha$ and hence $x^{15} = 1$. Hence period of $m(x)$ and A are each equal to 15. *

In the following we take up the computation of period of A for the other three cases. Towards this end we first prove the following lemma.

Lemma 3.3.3:

Consider a $K \times K$ matrix A over $P_p^n[W(a)]$, where $W(a) = \prod_{i=1}^{\nu} W_i^{h_i}(a)$, and $W_i(a)$, $i=1, \dots, \nu$ are irreducible polynomials over $GF(p)$. Then

$$|A| \text{ modulo } [p; W_i(a)] = |A \text{ modulo } [p; W_i(a)]| \Delta |\tilde{A}_i|; i=1, \dots, \nu.$$

Proof:

$|A|$ is algebraic sum of $K!$ terms constructed in the following manner. The terms are all possible products of the K elements of the matrix taken one in each row and each column; the term having a plus sign if its subscripts form an even permutation and a minus sign otherwise [76].

A typical term in the summation is

$$\begin{aligned}
 & (a_0, \alpha_0, a_1, \alpha_1, a_2, \alpha_2, \dots, a_{K-1}, \alpha_{K-1}) \text{ where } (\alpha_0, \alpha_1, \dots, \alpha_{K-1}) \text{ is a} \\
 & \text{permutation of the } K \text{ elements } (0, 1, \dots, K-1). \text{ We have} \\
 & (a_0, \alpha_0, a_1, \alpha_1, \dots, a_{K-1}, \alpha_{K-1}) \text{ modulo } [p; W_i(a)] \\
 & = (a_0, \alpha_0 \text{ modulo } [p; W_i(a)])(a_1, \alpha_1 \text{ modulo } [p; W_i(a)]) \dots \\
 & (a_{K-1}, \alpha_{K-1} \text{ modulo } [p; W_i(a)])
 \end{aligned}$$

Since $|A|$ is a sum of $K!$ such terms we have

$$|A| \text{ modulo } [p; W_i(a)] = |A \text{ modulo } [p; W_i(a)]| = |\tilde{A}_i|. *$$

As we have seen in Section 2.4, if an element is a unit in $P_p^n[W(a)]$, its external direct sum components are also units (nonzero elements over $P_p^n[W_i(a)]$). If an element in $P_p^n[W(a)]$ is a zero divisor, then in the external direct sum components at least one component is a nonunit. (zero element over $P_p^n[W_i(a)]$). Thus if $|A|$ is a unit in $P_p^n[W(a)]$, then the component $|\tilde{A}_i|$ is a unit in $P_p^n[W_i(a)]$, $i=1, \dots, \nu$. If $|A|$ is a zero divisor in $P_p^n[W(a)]$, at least one component $|\tilde{A}_i|$ $i=1, \dots, \nu$ is a zero. Thus if A is nonsingular its external direct sum components are also nonsingular.

ii) $W(a) = W_1^h(a)$; $W_1(a)$ is an irreducible polynomial of degree n_1 over $GF(p)$ and hence A is over a local ring of order p^n ; $n = hn_1$.

$$\text{Let } A = \begin{bmatrix} a_{00} & \cdots & a_{0,K-1} \\ \vdots & \ddots & \vdots \\ a_{K-1,0} & \cdots & a_{K-1,K-1} \end{bmatrix}; a_{ij} \in P_p^n[w(a)].$$

We define $\tilde{A} \triangleq A \text{ modulo } [p; W_i(a)]$

$$= \begin{bmatrix} a_{0,0} \text{ modulo } [p; W_i(a)] & \cdots & a_{0,K-1} \text{ modulo } [p; W_i(a)] \\ a_{K-1,0} \text{ modulo } [p; W_i(a)] & \cdots & a_{K-1,K-1} \text{ modulo } [p; W_i(a)] \end{bmatrix}$$

\tilde{A} is over a finite field of order p^{n_i} and the determination of the period of such a matrix has been already discussed in case (i). We now show that the period of the characteristic matrix A is determined in terms of the period of \tilde{A} and the integer h . Towards this end we first prove the following Lemma.

Lemma 3.3.4:

Let A be a $K \times K$ matrix with elements from $P_p^n[W_i^h(a)]$, where $W_i(a)$ is an irreducible polynomial over $GF(p)$. Then

$$\tilde{A}^\beta = A^\beta \text{ modulo } [p; W_i(a)], \text{ where } \beta \text{ is any integer.}$$

Proof:

We denote the $K \times K$ matrix $A \triangleq (a_{ij})$; $a_{ij} \in P_p^n[W_i^h(a)]$.

Since $\tilde{A} = A \text{ modulo } [p; W_i(a)]$

$$\tilde{A} \triangleq (a_{ij} \text{ modulo } [p; W_i(a)])$$

$$\begin{aligned}
\text{Consider } \tilde{A}^2 &= (\sum_K (a_{iK} \text{ modulo } [p; W_1(a)])(a_{Kj} \text{ modulo } [p; W_1(a)])) \\
&= (\sum_K a_{iK} a_{Kj} \text{ modulo } [p; W_1(a)]) \\
&= (\sum_K a_{iK} a_{Kj}) \text{ modulo } [p; W_1(a)] \\
&= A^2 \text{ modulo } [p; W_1(a)].
\end{aligned}$$

In general it can be shown that

$$\tilde{A}^\beta = [A \text{ modulo } [p; W_1(a)]]^\beta = A^\beta \text{ modulo } [p; W_1(a)]. \quad *$$

Theorem 3.3.4:

Let A be a $K \times K$ nonsingular matrix with elements from $p_p^n[W_1^h(a)]$, where $W_1(a)$ is irreducible over $GF(p)$. Let integer j be such that, $p^{j-1} < h \leq p^j$. If period of \tilde{A} is T , that is if $\tilde{A}^T = I \text{ modulo } [p; W_1(a)]$, then $A^{p^j T} = I \text{ modulo } [p; W_1^h(a)]$.

Proof:

From Lemma 3.3.3 if A is nonsingular \tilde{A} is also nonsingular.

$$\tilde{A}^T = I \text{ modulo } [p; W_1(a)]$$

$$\text{i.e. } [A \text{ modulo } [p; W_1(a)]]^T = I \text{ modulo } [p; W_1(a)]$$

From the result of the Lemma 3.3.4 we have

$$A^T \text{ modulo } [p; W_1(a)] = I \text{ modulo } [p; W_1(a)]$$

$$\text{i.e. } A^T = I \text{ modulo } [p; W_1(a)]$$

This implies that A^T is of the form

$$A^T = I + W_i(a) \cdot B$$

where B is a $K \times K$ matrix with elements from $P_p^{n_i}[W_i(a)]$.

$$\text{Hence } [A^T]^{p^j} = I + W_i^{p^j}(a) \cdot B^{p^j}$$

Since $p^{j-1} < h \leq p^j$, $W_i^{p^j}(a)$ is a multiple of $W_i^h(a)$. Hence

$$[A^T]^{p^j} = A^{p^j T} = I \text{ modulo } [p; W_i^h(a)]. \quad *$$

$\tilde{A} = A \text{ modulo } [p; W_i(a)]$ has elements from finite field. Its period T can be computed using the results for case (i). From the results of Theorem 3.3.4, we have period of A modulo $[p; W_i^h(a)]$ equal to $p^j T$, where $p^{j-1} < h \leq p^j$.

Example 3.3.10:

$$\text{Consider } A = \begin{bmatrix} 1+a & 1 \\ a & 1+a \end{bmatrix} \text{ over } P_2^3[a^3+a^2+a+1]$$

We have, $W(a) = (a+1)^3$. Hence $W(a) = (a+1)$ and $h = 3$.

$$\tilde{A} = A \text{ modulo } [2; a+1] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\tilde{A}^2 = I \text{ modulo } [2; a+1]. \text{ Hence } T = 2$$

$$\text{and } 2^1 < 3 < 2^2$$

Therefore period of A modulo $[2; a^3+a^2+a+1]$ is $4 \cdot 2 = 8$.

Example 3.3.11:

$$\text{Let } A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix} \text{ be over } P_2^{16} [a^{16}+1].$$

$(a^{16}+1) = (a+1)^{2^4}$. Hence $w_1(a)=(a+1)$ and $h = 16$.

A modulo $[2; a+1] = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

Period of A modulo $[2, a+1]$ is 3

and $2^3 < 16 = 2^4$

Therefore period of A is $2^4 \times 3 = 48$.

We now consider case (iii)

iii) $W(a)$ is a product of distinct irreducible polynomials:

A is over semisimple ring. Let $W(a) = \prod_{i=1}^v W_i(a)$;

$W_i(a)$ is n_i th-degree irreducible polynomial over $GF(p)$ and

$\sum_{i=1}^v n_i = n = \text{the degree of } W(a)$.

We have seen in Section 2.3, that for this case the ring $P_p^n[W(a)]$ is the internal direct sum of ideals J_1, J_2, \dots, J_v , generated by the orthogonal idempotents $e_1(a), e_2(a), \dots, e_v(a)$ respectively. Each element $r(a) \in P_p^n[W(a)]$ can be written as a unique sum

$$r(a) = r_1(a) + r_2(a) + \dots + r_v(a) \text{ modulo } [p; W(a)]$$

(3.3.7)

where $r_i(a) \in J_i$ and is a multiple of $e_i(a)$; $i=1,2,\dots,\nu$

and $J_i \simeq P_p^{n_i}[W_i(a)]$ ^{If} $r(a) = 0 \in P_p^n[W(a)]$. Then

$$r_i(a) = 0 \in J_i, \quad \forall i = 1, 2, \dots, \nu$$

As a consequence, A over $P_p^n[W(a)]$ can be written as internal direct sum of ν matrices.

$$A = A_1 + A_2 + \dots + A_\nu \text{ modulo } [p; W(a)]$$

where the elements of $K \times K$ matrix A_i are from J_i ; $i=1,2,\dots,\nu$

Consider one of the components A_i of A . The elements of A_i are from ideal J_i and hence the determinant of A_i is an element from J_i and hence a zero divisor. Although the matrix is singular, since the order of J_i is finite, as we list powers of A_i there will be repetition. If there exists an integer T_i , such that

$$A_i^{T_i} = \begin{bmatrix} e_i(a) & & 0 \\ & \ddots & \\ 0 & & e_i(a) \end{bmatrix} \quad (3.3.8)$$

We call T_i pseudo period of A_i

Since $e_i(a)$ is an orthogonal idempotent, $e_i(a) \cdot e_i(a) = e_i(a)$

$$\text{Hence } A_i^{T_i} = A_i^{jT_i} = \begin{bmatrix} e_i(a) & \dots & 0 \\ & \ddots & \\ 0 & \dots & e_i(a) \end{bmatrix} \text{ for all integer } j > 0.$$

We shall obtain a relationship between the period of A and the pseudo periods of components A_1, A_2, \dots, A_ν . Towards this end, we first prove the following.

Theorem 3.3.5:

Let $A = A_1 + A_2 + \dots + A_\nu$ be the internal direct sum decomposition of matrix A , Then

$$A^m = A_1^m + A_2^m + \dots + A_\nu^m$$

Proof:

We prove the theorem by induction on ν . The theorem is true for $\nu = 1$.

Since $A = A_1$, this implies $A^m = A_1^m$ modulo $[p; W(a)]$.

For $\nu = 2$ we have

$$A = A_1 + A_2 \text{ modulo } [p; W(a)]$$

$$\text{Now } A^m = (A_1 + A_2)^m$$

$$= A_1^m + \binom{m}{1} A_1^{m-1} A_2 + \dots + \binom{m}{m'} A_1^{m-m'} A_2^{m'} + \dots$$

$$\binom{m}{m-1} A_1 A_2^{m-1} + A_2^m$$

where,

$$\binom{m}{i} = \frac{m!}{(m-i)!i!}$$

Elements of A_1 are multiples of $e_1(a)$ and elements of A_2 are multiples of $e_2(a)$. Since $e_1(a)$ and $e_2(a)$ are orthogonal idempotents in $P_p^n[W(a)]$, $e_1(a) \cdot e_2(a) = 0$ modulo $[p; W(a)]$. Hence all the products $A_1^{m-m'} A_2^{m'} = \underline{0}$ modulo $[p; W(a)]$ for all $m' \neq m$.

$$\text{Therefore, } A^m = A_1^m + A_2^m$$

The theorem is true for $\nu = 2$.

Suppose the theorem holds good for $\nu-1$ i.e. $(A_1 + A_2 + \dots + A_{\nu-1})^m = A_1^m + \dots + A_{\nu-1}^m$, we show that it holds good for ν .

$$\begin{aligned} A^m &= [(A_1 + A_2 + \dots + A_{\nu-1}) + A_\nu]^m \text{ modulo } [p; W(a)] \\ &= [(A_1 + A_2 + \dots + A_{\nu-1})^m + A_\nu^m] \text{ modulo } [p; W(a)] \\ &= [A_1^m + A_2^m + \dots + A_{\nu-1}^m + A_\nu^m] \text{ modulo } [p; W(a)] \end{aligned} \quad *$$

We consider the relation between the period of A and the period of its components A_1, A_2, \dots, A_ν .

When A is nonsingular, there exists a least integer T such that, $A^T = I_{K \times K}$. We have seen in Section 2.4, that $e_1(a) + e_2(a) + \dots + e_\nu(a) = 1$ modulo $[p; W(a)]$. Also from (3.3.8) we see that the off diagonal terms in A_i^T are zero $i = 1, 2, \dots, \nu$

Hence,

$$A^T = \begin{bmatrix} e_1(a) & & 0 \\ & e_1(a) & \\ 0 & & 0 \\ \vdots & & \\ 0 & & e_1(a) \end{bmatrix} + \begin{bmatrix} e_2(a) & 0 & 0 \\ & e_2(a) & 0 \\ 0 & & e_2(a) \end{bmatrix} + \dots +$$

$$\begin{aligned}
& + \begin{bmatrix} e_y(a) & . & . & . \\ . & . & e_y(a) & . \\ . & . & . & e_y(a) \end{bmatrix} \\
& = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & . & \dots & 1 \end{bmatrix} \quad \text{modulo } [p; w(a)]
\end{aligned}$$

From the results of the Theorem 3.3.5 we have,

$$A^T = [A_1^T + A_2^T + \dots + A_y^T] = I_{K \times K} \text{ modulo } [p; w(a)]$$

This implies that,

$$A_i^T = \begin{bmatrix} e_i(a) & & 0 \\ & e_i(a) & \\ 0 & & e_i(a) \end{bmatrix}$$

Let T_i be the least integer such that

$$A_i^{T_i} = \begin{bmatrix} e_i(a) & & 0 \\ & e_i(a) & \\ 0 & & e_i(a) \end{bmatrix}.$$

T_i is then the pseudo period of A_i ; $i=1,2,\dots,y$ and as seen earlier since $e_i^2(a) = e_i(a)$ we have $A_i^{T_i} = A_i^{jT_i}$; j any

integer > 0 . Thus when A is nonsingular the component A_i is strictly periodic. $i = 1, 2, \dots, \nu$.

We prove the following theorem which relates T and T_1, T_2, \dots, T_ν .

Theorem 3.3.6:

The period T of A is equal to the lcm of the pseudo periods T_1, T_2, \dots, T_ν of A_1, A_2, \dots, A_ν respectively.

Proof:

T is the least integer such that, $A^T = I_{K \times K}$ modulo $[p; W(a)]$. We have,

$$\begin{aligned} A^T &= I_{K \times K} = [A_1^T + A_2^T + \dots + A_\nu^T] \text{ modulo } [p; W(a)] \\ &= \begin{bmatrix} e_1(a) & 0 \\ 0 & e_1(a) \end{bmatrix} + \begin{bmatrix} e_2(a) & \dots & 0 \\ 0 & & e_2(a) \end{bmatrix} + \dots \\ &\quad + \begin{bmatrix} e_\nu(a) & 0 \\ 0 & e_\nu(a) \end{bmatrix} \text{ modulo } [p; W(a)] \end{aligned}$$

T_i is the pseudo period of A_i ; $i = 1, 2, \dots, \nu$.

It is the least integer such that,

$$A_i^{T_i} = \begin{bmatrix} e_i(a) & & 0 \\ & \ddots & \\ 0 & & e_i(a) \end{bmatrix} \text{ modulo } [p; w(a)]; \quad i=1,2,\dots,\nu$$

but

$$A_i^T = \begin{bmatrix} e_i(a) & & 0 \\ & \ddots & \\ 0 & & e_i(a) \end{bmatrix} \text{ modulo } [p; w(a)]; \quad i = 1,2,\dots,\nu.$$

Therefore, $T_i | T$ $i = 1,2,\dots,\nu$.

The least integer T such that, $T_i | T$ for all $i = 1,2,\dots,\nu$ is the lcm of $T_1 T_2 \dots T_\nu$.

Hence the proof. *

We illustrate the application of Theorem 3.3.6 in computing the period of A in the following example.

Example 3.3.12:

$$\text{Let } A = \begin{bmatrix} a^2 & 1+a \\ 1+a+a^2 & a \end{bmatrix} \text{ be over } F_2^3[a^3+1].$$

$|A| = a^2 \cdot a + (1+a) \cdot (1+a+a^2) = 1$ modulo $[2; a^3+1]$, which is a unit in $F_2^3[a^3+1]$. Hence A is nonsingular. We first compute the period of A by computing its powers.

$$A^2 = \begin{bmatrix} a^2 & 1+a \\ 1+a+a^2 & a \end{bmatrix} \begin{bmatrix} a^2 & 1+a \\ 1+a+a^2 & a \end{bmatrix} = \begin{bmatrix} a & 1+a \\ 0 & a^2 \end{bmatrix} \text{ modulo } [2; a^3+1]$$

$$A^6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ modulo } [2; a^3+1]; \text{ thus period of } A \text{ is } 6.$$

We have seen in Example 2.3.1, that $P_2^3[a^3+1] = J_1 + J_2 = (a^2+a+1) + (a^2+a)$ where $(a^2+a+1) = e_1(a)$ and $(a^2+a) = e_2(a)$ are the orthogonal idempotents. Thus matrix A can be decomposed into its internal direct sum components

$A = A_1 + A_2 = e_1(a) A + e_2(a) A$. That is,

$$A = \begin{bmatrix} 1+a+a^2 & 0 \\ 1+a+a^2 & 1+a+a^2 \end{bmatrix} + \begin{bmatrix} 1+a & 1+a \\ 0 & 1+a^2 \end{bmatrix} \text{ modulo } [2; a^3+1]$$

where A_1 has elements from ideal, $J_1 = \langle a^2+a+1 \rangle$ and

A_2 has elements from ideal, $J_2 = \langle a^2+a \rangle$.

$$\begin{aligned} \text{Since } A_1^2 &= \begin{bmatrix} 1+a+a^2 & 0 \\ 0 & 1+a+a^2 \end{bmatrix} \text{ modulo } [2; a^3+1] \\ &= \begin{bmatrix} e_1(a) & 0 \\ 0 & e_1(a) \end{bmatrix} \end{aligned}$$

Pseudo period of A_1 is 2. Similarly,

$$A_2^3 = \begin{bmatrix} a+a^2 & 0 \\ 0 & a+a^2 \end{bmatrix} \text{ modulo } [2; a^3+1] = \begin{bmatrix} e_2(a) & 0 \\ 0 & e_2(a) \end{bmatrix}$$

Hence pseudo period of A_2 is 3.

Period of A is $\text{lcm}(2,3) = 6$, as obtained earlier by computing powers of A . *

In the internal direct sum decomposition of the ring $P_p^n[W(a)]$, since the summands are ideals in $P_p^n[W(a)]$, the elements of each summand belong to $P_p^n[W(a)]$. In the decomposition of A , the elements of the matrices A_1, A_2, \dots, A_ν belong to the ideals J_1, J_2, \dots, J_ν respectively and hence are zero divisors. Hence the technique developed for finding the minimal polynomial and hence period of A over finite field is not applicable here. For matrices of small size over ring of small order, it is possible to obtain the periods of A_i ; by taking powers of A_i $i=1,2,\dots,\nu$, as illustrated in the Example (3.3.12). However, when the size of the matrix and the order of the residue class polynomial ring over which it is defined are large, computing of powers of matrix A_i with elements from the ideal J_i , involves multiplication and addition of elements from J_i and then reducing to $W(a)$. Though the order of the ideal J_i is smaller than the ring $P_p^n[W(a)]$, the elements of J_i are from the same ring $P_p^n[W(a)]$, and hence are of degree $n-1$ or less. Hence the above procedure of computing period of A is not simple. We will see now that the computation of period of A is simplified by

considering the external direct sum decomposition of $P_p^n[W(a)]$. Since $W(a)$ is a product of irreducible polynomials over $GF(p)$ the external direct sum components of $P_p^n[W(a)]$ are finite fields. The corresponding decomposition of A , will have direct sum components of matrices over these finite fields. In a component of A the elements are from a finite field of order less than p^n , and hence the elements of component of A are polynomials whose degrees are less than $n-1$. For determining the period of any component of A , the procedure discussed in (i) can be adopted.

We have seen in Section 2.4, that

$$P_p^n[W(a)] \simeq P_p^{n_1}[W_1(a)] \oplus \dots \oplus P_p^{n_\nu}[W_\nu(a)]$$

and $P_p^{n_i}[W_i(a)] \simeq J_i$

We note here that $W_i(a)$ is irreducible over $GF(2)$; $i=1,2,\dots,\nu$. The external direct sum decomposition gives rise to a one to one correspondence between a $K \times K$ matrix A over $P_p^n[W(a)]$ and ν -tuple of $K \times K$ matrices

$$[\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_\nu]$$

where $\tilde{A}_i = A_i$ modulo $[p; W_i(a)]$ has elements from $P_p^{n_i}[W_i(a)]$. The period of A is obtained in terms of the periods of its components. Towards this end the following Lemma is proved.

Lemma 3.3.5:

$$\tilde{A}_i = A_i \text{ modulo } [p; W_i(a)] = A \text{ modulo } [p; W_i(a)].$$

Proof:

We have $A = A_1 + A_2 + \dots + A_\nu$, internal direct sum where A_i has elements from the ideal $\langle e_i(a) \rangle$ that is elements of A_i are multiples of $e_i(a)$. Since $e_i(a)$ is an orthogonal idempotent as seen in Section 2.3 it has

$$\prod_{\substack{j=1 \\ j \neq i}}^{\nu} W_j(a) \text{ as a factor}$$

Hence $A \text{ modulo } [p; W_i(a)] = [A_1 + A_2 + \dots + A_i + \dots + A_\nu] \text{ modulo } [p; W_i(a)]$.
 $W_i(a)$ is a factor of the matrices A_j ; $\forall j \neq i$, hence,

$$A \text{ modulo } [p; W_i(a)] = A_i \text{ modulo } [p; W_i(a)] = \tilde{A}_i.$$

And in general,

$$\tilde{A}_i = A \text{ modulo } [p; W_i(a)] \quad i = 1, 2, \dots, \nu.$$

Since $J_i \cong P_p^{n_i}[W_i(a)]$, there is a one-to-one correspondence between the internal and external direct sum components of A .

$$A_i \cong \tilde{A}_i \quad ; \quad i = 1, 2, \dots, \nu.$$

This implies that if T_i is the least integer such that

$$A_i^{T_i} = \begin{bmatrix} e_i(a) & & 0 \\ & \ddots & \\ 0 & & e_i(a) \end{bmatrix}$$

$$\text{Then } \tilde{A}_i^{T_i} = I_{K \times K}$$

That is the pseudo period of A_i and period of \tilde{A}_i are same and is equal to T_i .

Since $W_i(a)$ is irreducible over $GF(p)$; $P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$. The elements of \tilde{A}_i are from finite field $GF(p^{n_i})$ and the period of each component \tilde{A}_i $i=1,2,\dots,\nu$ can be determined as discussed in (i). Period of A is obtained in the following Theorem.

We prove the following theorem

*

Theorem 3.3.7:

Let $W(a) = \prod_{i=1}^{\nu} W_i(a)$, where $W_i(a)$; $i = 1,2,\dots,\nu$ is irreducible over $GF(p)$. Let A be a nonsingular matrix over $P_p^n[W(a)]$. Let $\tilde{A}_i = A$ modulo $[p; W_i(a)]$ and period of \tilde{A}_i be T_i $i = 1,2,\dots,\nu$. Then the period of A is $\text{lcm}(T_1, T_2, \dots, T_\nu)$.

Proof:

Proof follows from the results of Theorem 3.3.6 and the one to one correspondence between A_i and \tilde{A}_i .

Example 3.3.13:

Consider $A = \begin{bmatrix} 1+a & 1 \\ a & a \end{bmatrix}$ over $P_2^6[(a^3+a^2+1)(a^3+a+1)]$.

$$\tilde{A}_1 = A \text{ mod}[2; a^3+a^2+1] = \begin{bmatrix} 1+a & 1 \\ a & a \end{bmatrix}.$$

The minimal polynomial of \tilde{A}_1 is x^2+x+a which is primitive over $P_2^3[a^3+a^2+1] \simeq GF(2^3)$.

Hence period of $\tilde{A}_1 = (2^3)^2 - 1 = 63$.

$$\tilde{A}_2 = A \text{ modulo } [2; a^3+a+1] = \begin{bmatrix} 1+a & 1 \\ a & a \end{bmatrix}$$

whose minimal polynomial is x^2+x+a which is primitive over $P_2^3[a^3+a+1] \simeq GF(2^3)$. Hence period of \tilde{A}_2 is also = 63.

Period of $A = \text{lcm}(63, 63) = 63$.

Example 3.3.14:

Consider the ring $P_2^3[a^3+1]$ of Example 3.3.12; we have

$$P_2^3[a^3+1] \simeq P_2^1[a+1] \oplus P_2^2[a^2+a+1] \text{ and } A = \begin{bmatrix} a^2 & 1+a \\ 1+a+a^2 & a \end{bmatrix}$$

$$\tilde{A}_1 = A \text{ modulo } [2; a+1] = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

whose minimal polynomial is (x^2+1) over $GF(2)$. The period of $m(x) = 2$. Hence period of $\tilde{A}_1 = 2$. The period can also be found by taking powers of a_1 .

$$\tilde{A}_1^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ modulo } [2; a+1].$$

$$\tilde{A}_2 = A \text{ modulo } [2; a^2+a+1] = \begin{bmatrix} 1+a & 1+a \\ 0 & a \end{bmatrix} \text{ modulo } [2; a^2+a+1]$$

Minimal polynomial of \tilde{A}_2 is $(x+a^2)(x+a)$ modulo $[2; a^2+a+1] = x^2+x+1$, whose period is 3. Period can also be found by taking power of \tilde{A}_2 .

We have $\tilde{A}_2^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ modulo $[2; a^2+a+1]$.

Period of A_i and \tilde{A}_i ; $i=1,2$ are same.

Period of $A = \text{lcm}(2,3) = 6$.

*

iv) $W(a)$ is a product of powers of irreducible polynomials over $\text{GF}(p)$ i.e. A is over semilocal ring.

$$\text{Let } W(a) = \prod_{i=1}^{\nu} W_i^{h_i}(a)$$

where $W_i(a)$ is an n_i th degree irreducible polynomial over $\text{GF}(p)$, and $\sum_{i=1}^{\nu} n_i h_i = n = \text{the degree of } W(a)$.

We have seen in Section 2.3 that

$$\begin{aligned} P_p^n[W(a)] &\simeq P_p^{h_1 n_1}[W_1^{h_1}(a)] \oplus P_p^{h_2 n_2}[W_2^{h_2}(a)] \oplus \dots \\ &\oplus P_p^{h_{\nu} n_{\nu}}[W_{\nu}^{h_{\nu}}(a)] \dots \end{aligned}$$

This external direct sum decomposition of $P_p^n[W(a)]$ gives rise to a one-to-one correspondence between a $K \times K$ matrix A over $P_p^n[W(a)]$ and ν -tuple of $K \times K$ matrices $[A_1^*, A_2^*, \dots, A_{\nu}^*]$, where $A_i^* \triangleq A$ modulo $[p; W_i^{h_i}(a)]$ and has elements from $P_p^{h_i n_i}[W_i^{h_i}(a)]$ $i=1,2,\dots,\nu$. The period T_i of A_i^* can be computed using the results of case (ii). The period T of A is therefore given by $T = \text{lcm}(T_1, T_2, \dots, T_{\nu})$.

Example 3.3.15:

Consider $A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ over $P_2^6 [a^6+1]$ we have
 $(a^6+1) = (a+1)^2(a^2+a+1)^2$, Hence $P_2^6[a^6+1] \simeq P_2^2[a^2+1] \oplus P_2^4[a^4+a^2+1]$. We find the period of A in terms of the periods of A_1^* and A_2^* $A_1^* = A$ modulo $[2; a^2+1] = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$. Since (a^2+1) is power of an irreducible polynomial $(a+1)$, we use the procedure discussed in case (ii) $\tilde{A}_1^* = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ modulo $[2; a+1] = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Period of \tilde{A}_1^* is 3 and hence period of A_1^* is $3 \times 2 = 6$.
 $A_2^* = A$ modulo $[2; (a^2+a+1)^2] = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$; $\tilde{A}_2^* = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ modulo $[2; a^2+a+1]$.

Period of $\tilde{A}_2^* = 15$. Hence period of $A_2^* = 30$.

Thus period of A is $\text{lcm}(6, 30) = 30$.

Example 3.3.16:

Consider $A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ over $P_2^{10} [a^{10}+1]$. We have
 $(a^{10}+1) = (a+1)^2 (a^4+a^3+a^2+a+1)^2$
 $P_2^{10} [a^{10}+1] \simeq P_2^2 [a^2+1] \oplus P_2^8 [(a^4+a^3+a^2+a+1)^2]$.

We find the period of A in terms of the periods A_1^* and A_2^*

$$A_1^* = A \text{ modulo } [2; a^2+1] = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$$

$\tilde{A}_1^* = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ modulo $[2; a+1]$. As computed in earlier example period of A_1^* is 3. Hence period of \tilde{A}_1^* is 6.

$$A_2^* = A \text{ modulo } [2; (a^4+a^3+a^2+a+1)^2] = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$$

$\tilde{A}_2^* = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ modulo $[2; (a^4+a^3+a^2+a+1)] = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ is over

$$P_2^4[a^4+a^3+a^2+a+1] = GF(2^4).$$

Minimal polynomial $m_2(x)$ of \tilde{A}_2^* is x^2+ax+a and is primitive over $GF(2^4)$.

Period of $m_2(x)$ is 255 and hence period of \tilde{A}_2^* is 255.

Period of A_2^* is 510.

Thus period of A is $\text{lcm}(6, 510) = 510$.

3.3.3 Decomposition of $P_p^n[W(a)]$ -LSS:

We have seen in Section 2.4 that if $P_p^n[W(a)]$ is a semisimple or a semilocal ring, $(W(a) = \prod_{i=1}^v W_i^{h_i}(a))$, it is equal to the internal direct sum of orthogonal ideals J_1, J_2, \dots, J_v in $P_p^n[W(a)]$ or isomorphic to external direct sum of primary rings; field or local rings. Gross properties of the ring $P_p^n[W(a)]$ depend on the properties of internal or external direct sum components. The decomposition of $P_p^n[W(a)]$ lead to the notion of decomposition of $P_p^n[W(a)]$ -LSS into component systems over orthogonal ideals or primary rings.

The notion of decomposition of LSS also, helps in implementing larger LSS over semisimple or semilocal rings in terms of LSS over smaller primary rings namely finite field or local rings; these LSS are properly interconnected.

Thus the analysis and implementation of $P_p^n[W(a)]$ -LSS is basically analysis and implementation of LSS over finite fields and local rings. The results of the analysis of systems over finite fields and local rings can then be extended to the systems over semisimple or semilocal rings.

Let L be a $P_p^n[W(a)]$ -LSS. L is completely characterised by the characterising matrices A, B, C and D over $P_p^n[W(a)]$. Each element of the matrices can be decomposed into ν elements in the orthogonal ideals. Thus A, B, C , and D can be expressed as direct sum of component matrices.

$$A = A_1 + A_2 + \dots + A_\nu$$

$$B = B_1 + B_2 + \dots + B_\nu$$

$$C = C_1 + C_2 + \dots + C_\nu$$

$$D = D_1 + D_2 + \dots + D_\nu$$

In the decomposition the order of the matrices are unaltered. But now they are over orthogonal ideals whose orders are less than p^n .

Like wise, if we decompose states x , input u and output y , L can be decomposed into systems L_1, L_2, \dots, L_ν over the orthogonal ideals, where the characterising matrices of L_i are A_i, B_i, C_i , and D_i . The given system L is then a direct sum of ν systems L_1, L_2, \dots, L_ν as given in Figure 3.3.1a.

The analysis of L can be carried out in terms of the systems L_1, L_2, \dots, L_ν and finally combined. This notion is used in the computation of period of matrix A and in the cycle length decomposition of states of LSS discussed in Section 4.2. Multiplication by orthogonal idempotents decompose the input u into components $u^{(1)}, u^{(2)} \dots u^{(\nu)}$ over $J_1, J_2 \dots J_\nu$. L_i is over J_i $i=1, 2 \dots \nu$. The output $y^{(i)}$ of system L_i $i=1, 2 \dots \nu$ are added modulo $[p; w(a)]$, which is a unique element y in $P_p^n[w(a)]$. The input output relations are maintained in the two systems. We note here that if a nonsingular $P_p^n[w(a)]$ -LSS is decomposed into component subsystems over orthogonal ideals, the characteristic matrix A_i of the component subsystems L_i , $i=1, 2, \dots, \nu$ is singular. However, we recall that A_i is strictly periodic with pseudo period T_i ; $i=1, 2, \dots, \nu$.

$P_p^n[w(a)]$ is also isomorphic to its external direct sum components.

$$P_p^n[w(a)] \simeq P_p^{h_1 n_1}[w_1(a)] \oplus P_p^{h_2 n_2}[w_2(a)] \oplus \dots \oplus P_p^{h_\nu n_\nu}[w_\nu(a)].$$

Consequently, the characterising matrices A, B, C and D can be expressed as ν -tuples,

$$A = [\tilde{A}_1, \tilde{A}_2, \tilde{A}_3 \quad \dots \quad \tilde{A}_\nu]$$

$$B = [\tilde{B}_1, \tilde{B}_2, \tilde{B}_3 \quad \dots \quad \tilde{B}_\nu]$$

$$C = [\tilde{C}_1, \tilde{C}_2, \dots \quad \dots \quad \tilde{C}_\nu]$$

$$D = [\tilde{D}_1, \tilde{D}_2 \quad \dots \quad \tilde{D}_\nu]$$

where $\tilde{A}_i, \tilde{B}_i, \tilde{C}_i, \tilde{D}_i$ are over $P_p^{h_i n_i}[W_i^{h_i}(a)]$.

$$\tilde{A}_i = A \text{ modulo } P_p^{h_i n_i}[W_i^{h_i}(a)].$$

We can regard that $\tilde{A}_i, \tilde{B}_i, \tilde{C}_i, \tilde{D}_i$ are characterising matrices of $P_p^{h_i n_i}[W_i^{h_i}(a)]$ -LSS, \tilde{L}_i . If $h_i=1$, then \tilde{L}_i is over $P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$.

Given system L can thus be decomposed into systems \tilde{L}_i , $i = 1, 2, \dots, \nu$ over local rings or finite field. Decomposing the state x input u and output y into external direct sum components,

$$x = [\tilde{x}^{(1)} \quad \dots \quad \tilde{x}^{(\nu)}]$$

$$u = [\tilde{u}^{(1)} \quad \dots \quad \tilde{u}^{(\nu)}]$$

$$y = [\tilde{y}^{(1)} \quad \dots \quad \tilde{y}^{(\nu)}] \text{ and}$$

the decomposed system L is as shown in Figure 3.3.1b.

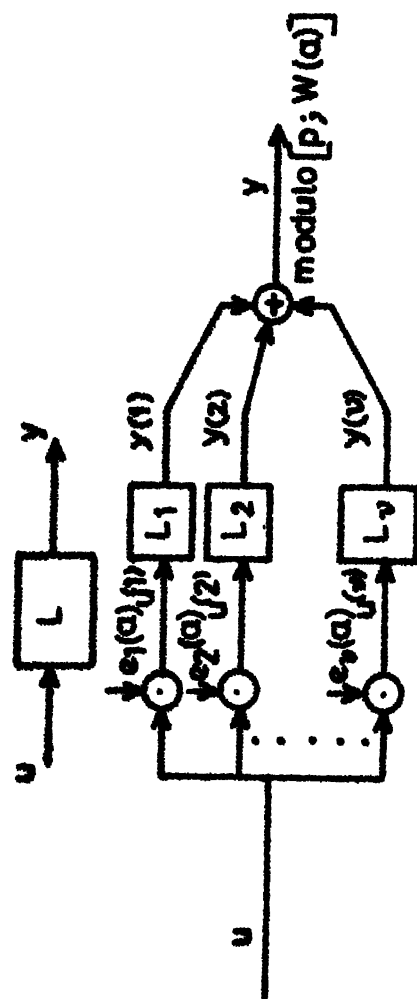


Fig. 3.3.1a Decomposition of $P_p^n [W(a)]$ -LSS L (based on internal direct sum)

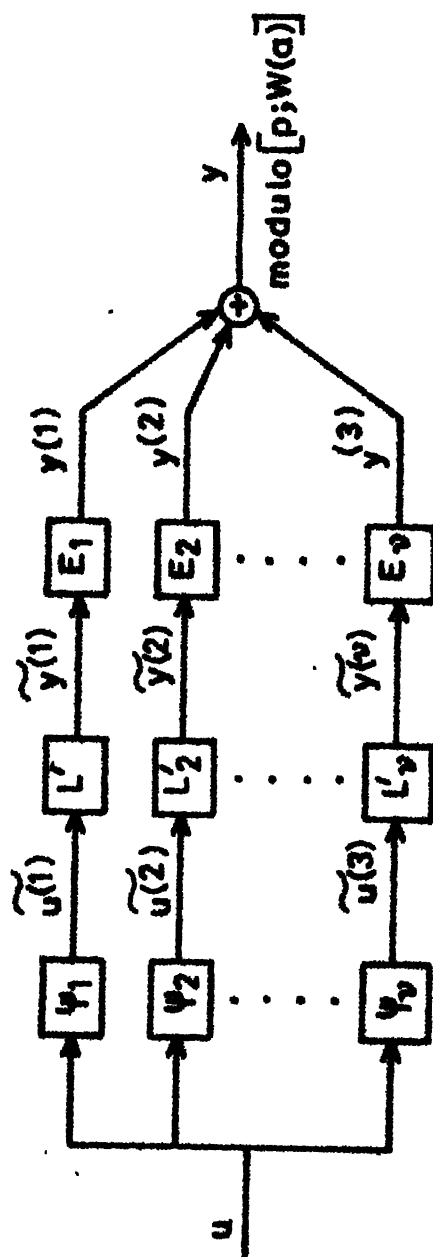


Fig. 3.3.1b Decomposition of $P_p^n [W(a)]$ -LSS L (based on external direct sum)

Ψ : is an isomorphism which maps an element $r(a)$ of $P_p^n[W(a)]$ to

$$P_p^{h_i n_i}[W_i^{h_i}(a)] ; \quad \tilde{u}^{(i)} = \underline{u} \text{ modulo } [p; W_i^{h_i}(a)]$$

$\tilde{y}^{(i)}$ is the output from the system $L_i^!$

E_i is the embedding which maps $\tilde{y}^{(i)}$ to the orthogonal ideal J_i in ring $P_p^n[W(a)]$.

The components $y^{(1)}, y^{(2)} \dots y^{(v)}$ are the internal direct sum components of the output y .

If $h_i = 1, \forall i$,

The system $L_i^!$, is over finite field $GF(p^{n_i})$. $i=1,2,\dots,v$.

Systems over semisimple or semilocal rings can be implemented by connecting modules of systems over finite field or local rings of smaller order with appropriate transformation networks at the input and output.

Examples 3.3.17:

Let L be a second order $P_2^3[a^3+1]$ -LSS

$$W_1(a) = (a+1), W_2(a) = (a^2+a+1)$$

$$\text{Let } A = \begin{bmatrix} 1+a^2 & 1 \\ a & 1+a+a^2 \end{bmatrix}; B = \begin{bmatrix} a^2 \\ 1 \end{bmatrix}; C = [1 \quad 1+a]; D=[a^2].$$

$|A| = a$, therefore, the system is nonsingular. In

this example,

$$e_1(a) = (a^2 + a + 1)$$

$$e_2(a) = (a^2 + a)$$

$$A_1 = \begin{bmatrix} 0 & 1+a+a^2 \\ 1+a+a^2 & 1+a+a^2 \end{bmatrix}; \quad A_2 = \begin{bmatrix} 1+a^2 & a+a^2 \\ 1+a^2 & 0 \end{bmatrix}$$

A_1, A_2 are singular over $P_2^3[a^3+1]$

$$B_1 = \begin{bmatrix} 1+a+a^2 \\ 1+a+a^2 \end{bmatrix}; \quad B_2 = \begin{bmatrix} 1+a \\ a+a^2 \end{bmatrix}$$

$$C_1 = [1+a+a^2, 0]; \quad C_2 = [a+a^2, 1+a]$$

$$D_1 = [1+a+a^2]; \quad D_2 = [1+a].$$

The decomposition of L is given in Figure 3.3.2a(internal direct sum).

The external direct sum components of the characterizing matrices are,

$$A'_1 = A \text{ modulo } [2; a+1] = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix};$$

$$A'_2 = A \text{ modulo } [2; a^2+a+1] = \begin{bmatrix} a & 1 \\ a & 0 \end{bmatrix}$$

Likewise $B'_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}; \quad B'_2 = \begin{bmatrix} 1+a \\ 1 \end{bmatrix}$

$$C'_1 = [1, 0]; \quad C'_2 = [1, 1+a]$$

$$D'_1 = [1]; \quad D'_2 = [1+a].$$

Decomposition of L (Ext. direct sum) is given in Fig. 3.3.2b.

L_1^1, L_2^1 are over finite field $GF(2)$ and $GF(2^2)$ respectively. Both are nonsingular systems.

Example 3.3.18:

Consider a 2nd order $P_2^3[a^3+1]$ -LSS, L with characterizing matrices

$$A = \begin{bmatrix} 1+a+a^2 & a \\ a & 1+a+a^2 \end{bmatrix}; B = \begin{bmatrix} a^2 \\ 1 \end{bmatrix}; C = [1 \quad 1+a]; D=[a^2]$$

$|A| = (a+1)$, a zero divisor in $P_2^3[a^3+1]$.

Hence the system is singular. Decomposing the matrices over J_1 and J_2 we have

$$A_1 = \begin{bmatrix} 1+a+a^2 & 1+a+a^2 \\ 1+a+a^2 & 1+a+a^2 \end{bmatrix}; A_2 = \begin{bmatrix} 0 & 1+a^2 \\ 1+a^2 & 0 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 1+a+a^2 \\ 1+a+a^2 \end{bmatrix}; B_2 = \begin{bmatrix} 1+a \\ a+a^2 \end{bmatrix}$$

$$C_1 = [1+a+a^2 \quad 0]; C_2 = [a+a^2 \quad 1+a]$$

$$D_1 = [1+a+a^2]; D_2 = [1+a]$$

The decomposition of L is given in Figure 3.3.3a.

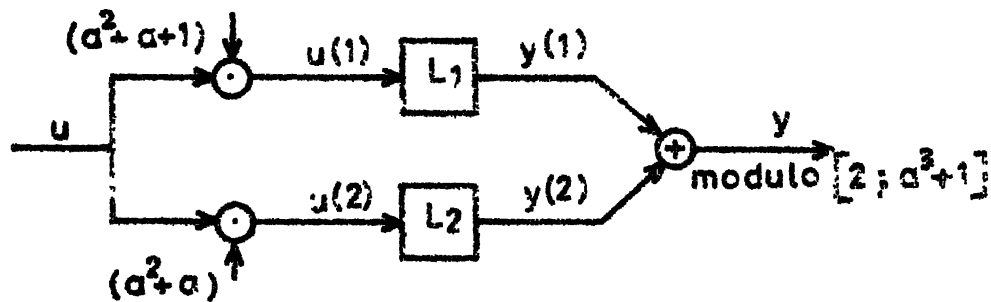


Fig. 3.3.2a Decomposition of $P_2^3[a^3+1]$ -LSS
of Example 3.2.7 (based on internal
direct sum)

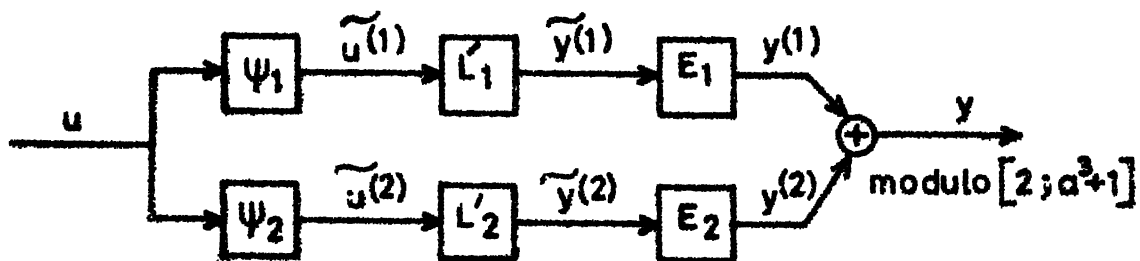


Fig. 3.3.2b Decomposition of $P_2^3[a^3+1]$ -LSS
of Example 3.2.7 (based on external
direct sum)

The external direct sum components of characterising matrices are

$$A_1' = A \text{ modulo } [2; (a+1)] = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix};$$

$$A_2' = A \text{ modulo } [2; a^2+a+1] = \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix}$$

Likewise

$$B_1' = \begin{bmatrix} 1 \\ 1 \end{bmatrix}; \quad B_2' = \begin{bmatrix} 1+a \\ 1 \end{bmatrix}$$

$$C_1' = [1 \ 0]; \quad C_2' = [1 \ 1+a]$$

$$D_1' = [1]; \quad D_2' = [1+a].$$

The decomposition of L (external direct sum) is given in Figure 3.3.3b.

L_1' is a singular system over $P_2^1[a+1] \simeq GF(2)$

L_2' is a nonsingular system over $P_2^2[a^2+a+1] \simeq GF(2^2)$.

3.4 LSS OVER OTHER FAMILIES OF FINITE COMMUTATIVE RINGS:

If the entries in Equations (3.1.1) and (3.1.2) are from a finite commutative ring other than $P_p^n[W(a)]$, then depending upon the specific finite commutative rings used, we obtain other families of LSS. In Section 2.2 we have defined tensor product of residue class polynomial rings which is a generalisation of $P_p^n[W(a)]$. Further in Section 2.3

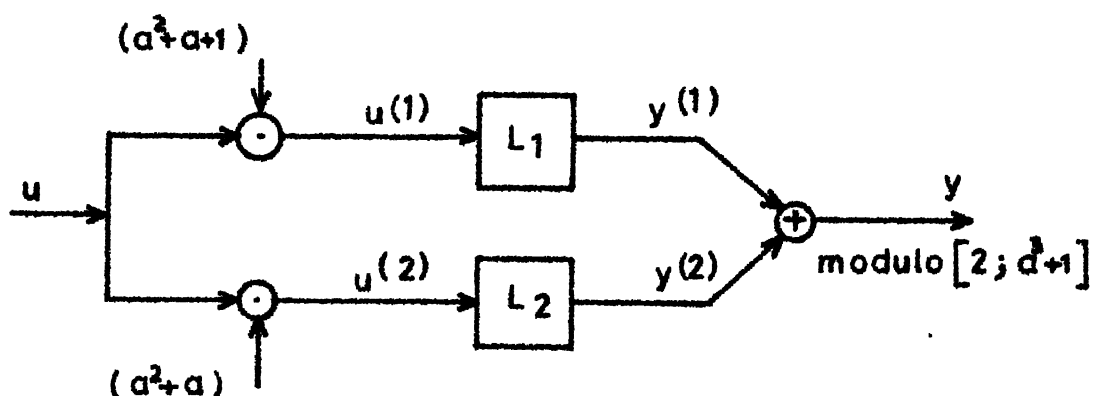


Fig.3.3.3a Decomposition of $P_2^3[a+1]$ -LSS
of Example 3.2.8
(based on internal directsum)

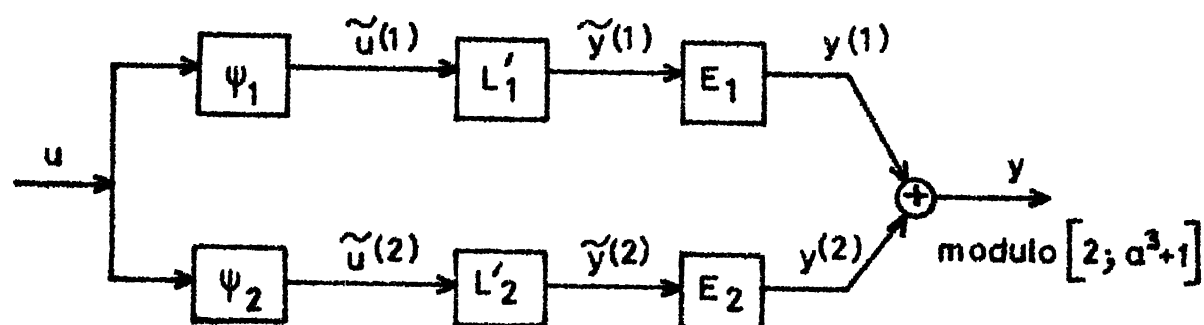


Fig.3.3.3b Decomposition of $P_2^3[a^3+1]$ -LSS
of Example 3.2.8
(based on external direct sum)

it is seen that, $\bigotimes^T \{P_p^{n_i}[w_i(a_i)]\}$ and $P_p^n[W(a)]$ are isomorphic to each other when there is a one-to-one correspondence between their bases which preserves the ring operations in the respective rings. In Section 2.6 we have obtained several families of isomorphic finite commutative rings. These include specifically ring $Z_p^n[W]$ of n -tuples, $M_p^n[W]$ of $n \times n$ commutative matrices isomorphic to $P_p^n[W(a)]$ and tensor product $\bigotimes^T \{Z_p^{n_i}[w_i]\}$ and $\bigotimes^T \{M_p^{n_i}[w_i]\}$ isomorphic to $\bigotimes^T \{P_p^{n_i}[w_i(a_i)]\}$. In this section we study LSS over these commutative rings. The notion of isomorphism between families of rings leads to the isomorphism between families of systems.

If two linear sequential systems defined over isomorphic rings are such that there is one-to-one correspondence between their characterising matrices and states then with isomorphic initial states and isomorphic input sequences the output sequences of the two LSS are isomorphic to each other. Such LSS are called isomorphic LSS. In this section we consider LSS defined over different isomorphic rings.

The ring Z_m of residue classes of integers modulo m in general is not isomorphic to $P_p^n[W(a)]$ except for the case $m=p$ and $n=1$; accordingly Z_m -LSS studied in [40] are not isomorphic to $P_p^n[W(a)]$ -LSS except for the case pointed out above.

Because of the isomorphisms between LSS over different rings, systems over one ring can be implemented and analysed in terms of systems over the other ring. For example $P_p^n[W(a)]$ -LSS can be implemented as $Z_p^n[W]$ -LSS, which as we shall see is a subclass of $GF(p)$ -LSS. The period of characteristic matrix A of LSS over semisimple or semilocal $Z_p^n[W]$ can be obtained in terms of period of characteristic matrix A of an isomorphic $P_p^n[W(a)]$ -LSS. Analysis of a subclass of $GF(p)$ -LSS of order nK which are essentially $Z_p^n[W]$ -LSS can be carried out in terms of $P_p^n[W(a)]$ -LSS of order K . Analysis of LSS over local $P_p^n[W(a)]$ can be carried out in terms of $Z_p^n[W]$ -LSS.

3.4.1 LSS Over Tensor Product $\bigotimes_{i=1}^T P_p^{n_i}[W_i(a_i)]$ of Residue Class Polynomial Rings:

In Section 2.2 we have seen that tensor product of two or more residue class polynomial rings denoted by $\bigotimes_{i=1}^T P_p^{n_i}[W_i(a_i)]$ has the structure of a finite commutative ring which constitutes a general class of residue class polynomial rings. LSS defined over tensor product of residue class polynomial rings are denoted by $\bigotimes_{i=1}^T P_p^{n_i}[W_i(a_i)]$ -LSS. The elements of characterising matrices, input sequence, output sequence and state sequence are then from $\bigotimes_{i=1}^T P_p^{n_i}[W_i(a_i)]$. Since residue class polynomial ring is also an algebra over $GF(p)$, it has a basis. If there is one-to-one correspondence ϕ between the

elements of the basis of $P_p^n[W(a)]$ and $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ which satisfies the conditions of Theorem 2.3.1 then $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ is isomorphic to $P_p^n[W(a)]$. Given a $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ -LSS, an isomorphic $\bigotimes^T P_p^n[W(a)]$ -LSS can be determined.

Example 3.4.1:

Consider a second order LSS over $P_2^2[a_1^2+a_1+1] \bigotimes^T P_2^2[a_0^2+1]$ described by

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1+a_1a_0 & a_0+a_1a_0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & a_1a_0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a_1a_0 \\ 1 \end{bmatrix} u$$

where x_0, x_1, y_0, y_1, u and the elements of the characterising matrices

$$A = \begin{bmatrix} 1+a_1a_0 & a_0+a_1a_0 \\ 1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}; \quad C = \begin{bmatrix} 1 & a_1a_0 \\ 1 & 0 \end{bmatrix}$$

and $D = \begin{bmatrix} a_1a_0 \\ 1 \end{bmatrix}$ are from $P_2^2[a_1^2+a+1] \bigotimes^T P_2^2[a_0^2+1]$.

Example 3.4.2:

As illustrated in Example (2.3.7), $P_2^3[a_1^3+1] \bigotimes^T P_2^2[a_0^2+1]$ is isomorphic to semilocal ring $P_2^6[a^6+1]$, with the one-to-one correspondence in their basis $1 \neq 1$, $a_1a_0 \neq a$, $a_1^2 \neq a^2$,

$a_0 \neq a^3$, $a_1 \neq a^4$, $a_1^2 a_0 \neq a^5$. Consider a second order LSS over $P_2^3[a_1^3+1] \otimes^T P_2^2[a_0^2+1]$ described by,

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1+a_1 a_0 & a_0+a_1 a_0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & a_1 a_0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a_1 a_0 \\ 1 \end{bmatrix} u$$

where $x_0, x_1, y_0, y_1, u \in P_2^3[a_1^3+1] \otimes^T P_2^2[a_0^2+1]$. The isomorphic LSS over $P_2^6[a^6+1]$ is described by

$$\begin{bmatrix} \theta'_0 \\ \theta'_1 \end{bmatrix} = \begin{bmatrix} 1+a & a+a^3 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} + \begin{bmatrix} a^3 \\ a^4 \end{bmatrix} \gamma$$

$$\begin{bmatrix} \delta_0 \\ \delta_1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} + \begin{bmatrix} a \\ 1 \end{bmatrix} \gamma$$

where $\theta_0, \theta_1, \delta_0, \delta_1, \gamma \in P_2^6[a^6+1]$.

3.4.2 LSS Over Ring $M_p^n[W]$ of nxn Commutative Matrices:

In Section 2.6 it is shown that a commutative ring of nxn matrices over $GF(p)$ isomorphic to a given residue class ring of polynomial of order p^n over $GF(p)$ exists. Procedures for construction of such matrix ring where zeroth column

of each matrix is equal to the column vector of coefficients of corresponding polynomial is also given. Using the isomorphism between the residue class polynomial rings and commutative rings of $n \times n$ matrices, we give the state and output equations of a LSS say L' over commutative ring of $n \times n$ matrices which is isomorphic to a given $P_p^n[W(a)]$ -LSS.

Referring to the state and output Equations (3.1.1) and (3.1.2), for a $P_p^n[W(a)]$ -LSS the elements of the characterising matrices, state, input and output are drawn from $P_p^n[W(a)]$. The LSS L' isomorphic to L has the following state and output equations, which is obtained after replacing each entry of equations of L by corresponding elements from commutative ring $M_p^n[W]$ of $n \times n$ matrices isomorphic to $P_p^n[W(a)]$. (The $n \times n$ submatrices are denoted by lower case letters with double bars below).

$$\begin{bmatrix} \underline{\underline{x}}_0(N+1) \\ \vdots \\ \underline{\underline{x}}_{K-1}(N+1) \end{bmatrix} = \begin{bmatrix} \underline{\underline{a}}_{0,0} & \cdots & \underline{\underline{a}}_{0,K-1} \\ \vdots & \ddots & \vdots \\ \underline{\underline{a}}_{K-1,0} & \cdots & \underline{\underline{a}}_{K-1,K-1} \end{bmatrix} \begin{bmatrix} \underline{\underline{x}}_0(N) \\ \vdots \\ \underline{\underline{x}}_{K-1}(N) \end{bmatrix} \\ + \begin{bmatrix} \underline{\underline{b}}_{0,0} & \cdots & \underline{\underline{b}}_{0,m-1} \\ \vdots & \ddots & \vdots \\ \underline{\underline{b}}_{K-1,0} & \cdots & \underline{\underline{b}}_{K-1,m-1} \end{bmatrix} \begin{bmatrix} \underline{\underline{u}}_0(N) \\ \vdots \\ \underline{\underline{u}}_{m-1}(N) \end{bmatrix}$$

$$\begin{bmatrix} \underline{y}_0(N) \\ \vdots \\ \underline{y}_{j-1}(N) \end{bmatrix} = \begin{bmatrix} \underline{c}_{0,0} & \cdots & \underline{c}_{0,K-1} \\ \vdots & & \\ \underline{c}_{j-1,0} & \cdots & \underline{c}_{j-1,K-1} \end{bmatrix} \begin{bmatrix} \underline{x}_0(N) \\ \vdots \\ \underline{x}_{K-1}(N) \end{bmatrix} \\
 + \begin{bmatrix} \underline{d}_{0,0} & \cdots & \underline{d}_{0,m-1} \\ \vdots & \ddots & \vdots \\ \underline{d}_{j-1,0} & \cdots & \underline{d}_{j-1,m-1} \end{bmatrix} \begin{bmatrix} \underline{u}_0(N) \\ \vdots \\ \underline{u}_{m-1}(N) \end{bmatrix}$$

Thus given an LSS of order K over residue class polynomial ring $P_p^n[W(a)]$, it is possible to obtain an isomorphic LSS of order K over an isomorphic commutative ring of $n \times n$ matrices. In this isomorphic system the input/output elements and $n \times n$ submatrices of the characterising matrices are from commutative ring $M_p^n[W]$ of $n \times n$ matrices isomorphic to $P_p^n[W(a)]$. $M_p^n[W]$ -LSS of order K are a subclass of $GF(p)$ -LSS of order nK . Such LSS can be analysed in terms of $P_p^n[W(a)]$ -LSS.

Example 3.4.3:

Consider the 1-input, 2-output second order LSS of Example 3.1.1 over local ring $P_2^2[a^2+1]$.

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1+a & a \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a \\ 1 \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 0 \\ a \end{bmatrix} u$$

LSS L' over $M_2^2 \simeq P_2^2[a^2+1]$ which is isomorphic to the above LSS is obtained by replacing a by the 2×2 matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and 1 by $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$$\begin{bmatrix} \underline{x}'_0 \\ \underline{x}'_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \underline{x}_0 \\ \underline{x}_1 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} [\underline{u}]$$

$$\begin{bmatrix} \underline{y}_0 \\ \underline{y}_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \underline{x}_0 \\ \underline{x}_1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} [\underline{u}]$$

where \underline{x}_i , \underline{u} , \underline{y}_i are 2×2 matrices from the commutative ring of 2×2 matrices M_2^2 isomorphic to $P_2^2[a^2+1]$. The input 2-tuple and output 2-tuple are arrays of 2×2 matrices from M_2^2 .

Example 3.4.4:

Consider a second order LSS over the local ring $P_2^3[a^3+a^2+a+1]$ of Example 2.6.2 with the following state and output equations.

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1+a+a^2 & 1+a \\ a^2 & 1+a^2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a^2 \\ 1+a^2 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & 1+a \\ a^2 & a+a^2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 1 \\ a \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}$$

This is a 2-input, 2-output second order LSS over $P_2^3[a^3+a^2+a+1]$.
 LSS L' over M_2^3 (isomorphic to $P_2^3[a^3+a^2+a+1]$), isomorphic to
 the above LSS is

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}$$

where x_i, u_i, y_i are 3×3 matrices from M_2^3 . The input 2-tuple
 and output 2-tuple are arrays of 3×3 matrices $\in M_2^3$.

Example 3.4.5:

Consider the semisimple rings $P_3^2[a^2-1]$. Let the state
 and output equations of a 2nd order LSS over $P_3^2[a^2-1]$ be

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1+2a & a \\ 2+a & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a \\ 2a \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 2a & a \\ 1 & 1+a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 1 \\ a \end{bmatrix} u$$

LSS L' over ring of 2×2 matrices over $GF(3)$ and isomorphic to the above LSS L is

$$\begin{bmatrix} \underline{x}_0' \\ \underline{x}_1' \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix} \begin{bmatrix} \underline{x}_0 \\ \underline{x}_1 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 2 \\ 2 & 0 \end{bmatrix} u$$

$$\begin{bmatrix} \underline{y}_0 \\ \underline{y}_1 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \underline{x}_0 \\ \underline{x}_1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} u$$

where x_i , u , y_i are 2×2 matrices from the commutative ring of 2×2 matrices M_3^2 isomorphic to $P_3^2 [a^2-1]$. The input and output 2-tuples are 2×2 matrices from M_3^2 .

3.4.3 LSS Over Tensor Product $\bigotimes_{i=1}^T \{M_p^{n_i} [W_i]\}$ of Commutative Ring of Matrices:

As in the previous case, given an LSS, L over $\bigotimes_{i=1}^T \{P_p^{n_i} [W_i(a_i)]\}$ it is possible to obtain an isomorphic LSS, L' over commutative ring, $\bigotimes_{i=1}^T \{M_p^{n_i} [W_i]\}$ of $n \times n$ matrices (isomorphic to $\bigotimes_{i=1}^T \{P_p^{n_i} [W_i(a_i)]\}$). In the state and output equations of L' the input/output elements and $n \times n$ submatrices

of the characterising matrices are from commutative ring $\bigotimes^T \{M_p^{n_i}[W_i]\}$ of $n \times n$ matrices isomorphic to $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$.

We illustrate with the following example.

Example 3.4.6:

Consider the second order LSS, L , of Example 3.4.1 over $P_2^2[a_1^2+a_1+1] \bigotimes^T P_2^2[a_0^2+1]$.

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1+a_1a_0 & a_0+a_1a_0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & a_1a_0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a_1a_0 \\ 1 \end{bmatrix} u$$

where $x_0, x_1, y_0, y_1, u \in P_2^2[a_1^2+a_1+1] \bigotimes^T P_2^2[a_0^2+1]$. LSS, L' , over $M_2^2[W_1] \bigotimes^T M_2^2[W_0]$, isomorphic to the above LSS, L is

$$\begin{bmatrix} \underline{x}'_0 \\ \underline{x}'_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \underline{x}_0 \\ \underline{x}_1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} u$$

$$\begin{bmatrix} \underline{y}_0 \\ \underline{y}_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \underline{x}_0 \\ \underline{x}_1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \underline{u}$$

Where $\underline{x}_0^1, \underline{x}_1^1, \underline{x}_0, \underline{x}_1, \underline{u}, \underline{y}_0, \underline{y}_1$ are 4×4 matrices from $M_2^2[W_1] \otimes M_2^2[W_0] \simeq P_2^2[a_1^2+a_1+1] \otimes P_2^2[a_0^2+1]$. The input and output 2-tuples are 4×4 matrices.

From the Examples 3.4.3 to 3.4.6 of $M_p^n[W]$ -LSS and $\bigotimes \{M_p^{n_i}[W_i]\}$ -LSS, we see that in these LSS, the $n \times n$ submatrices of characterising matrices and elements of input m -tuple and output j -tuple are from $M_p^n[W]$ and $\bigotimes \{M_p^{n_i}[W_i]\}$ respectively. These systems can be used to generate and process sequences of arrays over $GF(p)$ belonging to $M_p^n[W]$ or $\bigotimes \{M_p^{n_i}[W_i]\}$. It should be noted that these systems take care of only p^n , $n \times n$ arrays out of p^{n^2} possible arrays over $GF(p)$.

3.4.4 LSS Over Ring $Z_p^n[W]$ of n -tuples:

In Section 2.6 we have obtained ring of n -tuples, $Z_p^n[W]$ isomorphic to $P_p^n[W(a)]$. It is then straightforward

to obtain a LSS over $Z_p^n[W]$ -LSS $\simeq P_p^n[W(a)]$ -LSS. $Z_p^n[W]$ -LSS of order K are a subclass of $GF(p)$ -LSS of order nK .

In the state and output equations of $P_p^n[W(a)]$ -LSS, the computation of state involves the multiplication of elements of matrix A with the elements of states x and elements of B with elements of input u . Similarly computation of output involves the multiplication of elements of matrix C with elements of states x and elements of matrix D with elements of input u . Further all these elements are from $P_p^n[W(a)]$. In the ring of n -tuples $Z_p^n[W]$ isomorphic to $P_p^n[W(a)]$, the multiplication of two n -tuples is equal to the multiplication of an $n \times n$ matrix corresponding to one n -tuple and $n \times 1$ vector corresponding to the other n -tuple as discussed in Section 2.6. Hence in the state and output equations of $Z_p^n[W]$ -LSS, $L' \simeq P_p^n[W(a)]$ -LSS, L , the elements of the characterising matrices are appropriate $n \times n$ matrices over $GF(p)$ and the elements of state, input and output are appropriate n -tuples over $GF(p)$.

The following examples illustrate the procedure to obtain L' from L .

Example 3.4.7:

Consider the 1-input, 2-output second order LSS, L over local ring $P_2^2[a^2+1]$ of Example 3.1.1. The state and

output equations of LSS, L' isomorphic to LSS, L is obtained by replacing the elements of the characterising matrices by appropriate 2×2 matrices. The correspondence between the ring elements $P_2^2[a^2+1]$ and the 2×2 matrices over $GF(2)$ is given in Example 2.6.1.

The state and output equations of L' are

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} I_2 + W & W \\ I_2 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} W \\ I_2 \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} I_2 & W \\ I_2 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 0 \\ W \end{bmatrix} u$$

where I_2 is the 2×2 identity matrix and W is the companion matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ of (a^2+1) .

In the expanded form the equations are

$$\begin{bmatrix} x'_{00} \\ x'_{01} \\ x'_{10} \\ x'_{11} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{10} \\ x_{11} \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}$$

and

$$\begin{bmatrix} y_{00} \\ y_{01} \\ y_{10} \\ y_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{10} \\ x_{11} \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}$$

$x_{ij}, y_{ij}, u_i \in \text{GF}(2)$. The input sequence elements are 2-tuples and output sequence elements are 4-tuples. If the initial states of L and L' are isomorphic, then for isomorphic inputs, outputs are also isomorphic. L' can alternatively be interpreted as a 4th order $\text{GF}(2)$ -LSS.

Example 3.4.8:

Consider the 2-input 2-output second order LSS of Example 3.4.4 over the local ring, $P_2^3[a^3+a^2+a+1]$.

The state and output equations of L' are

$$\begin{bmatrix} \underline{x}'_0 \\ \underline{x}'_1 \end{bmatrix} = \begin{bmatrix} I_3 + W + W^2 & I_3 + W \\ W^2 & I_3 + W^2 \end{bmatrix} \begin{bmatrix} \underline{x}_0 \\ \underline{x}_1 \end{bmatrix} + \begin{bmatrix} W^2 \\ I_3 + W \end{bmatrix} u'$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} I_3 & I_3 + W \\ W^2 & W + W^2 \end{bmatrix} \begin{bmatrix} \underline{x}_0 \\ \underline{x}_1 \end{bmatrix} + \begin{bmatrix} I_3 \\ W^2 \end{bmatrix} u$$

where I_3 is the 3×3 identity matrix and W is the companion matrix $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ of $(a^3 + a^2 + a + 1)$ over $GF(2)$. In the expanded form the equations are

$$\begin{bmatrix} x'_{00} \\ x'_{01} \\ x'_{02} \\ x'_{10} \\ x'_{11} \\ x'_{12} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{02} \\ x_{10} \\ x_{11} \\ x_{12} \end{bmatrix} + \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \end{bmatrix}$$

$$\begin{bmatrix} y_{00} \\ y_{01} \\ y_{02} \\ y_{10} \\ y_{11} \\ y_{12} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{02} \\ x_{10} \\ x_{11} \\ x_{12} \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \end{bmatrix}$$

where $x_{ij}, y_{ij}, u_{ij} \in GF(2)$. The input sequence elements are 3-tuples and output sequence elements are 6-tuples over $GF(2)$.

If the initial states of L and L' are isomorphic, then for isomorphic inputs, outputs are also isomorphic. *

Example 3.4.9:

Consider the 2nd order, 1-input 2-output LSS of Example 3.4.5 over the semisimple ring, $P_3^2[a^2-1]$.

The state and output equations of L' are

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} I_2 + 2W & W \\ 2I_2 + W & I_2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} W \\ 2W \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 2W & W \\ I_2 & I_2 + W \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} I_2 \\ W \end{bmatrix} u$$

where I_2 is the 2×2 identity matrix and W is the companion matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ of $(a^2 - 1)$, over $GF(3)$.

In the expanded form the equations are

$$\begin{bmatrix} x'_{00} \\ x'_{01} \\ x'_{10} \\ x'_{11} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{10} \\ x_{11} \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 2 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}$$

$$\begin{bmatrix} y_{00} \\ y_{01} \\ y_{10} \\ y_{11} \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{10} \\ x_{11} \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}$$

where $x_{ij}, y_{ij}, u_i \in GF(2)$. The input sequence elements are 2-tuples and output sequence elements are 4-tuples over $GF(3)$.

If the initial states of L and L' are isomorphic, then for

isomorphic inputs outputs are also isomorphic. L' is a 4th order LSS over $GF(3)$.

3.4.5 LSS over Tensor Product $\bigotimes_{i=1}^T \{Z_p^{n_i}[W_i]\}$ of ring of n -tuples:

The isomorphism between $\bigotimes_{i=1}^T \{Z_p^{n_i}[W_i]\}$ and $\bigotimes_{i=1}^T \{P_p^{n_i}[W_i(a_i)]\}$ is established in Section 2.6. Hence as in the case of $Z_p^n[W]$ -LSS, it is possible to obtain $\bigotimes_{i=1}^T Z_p^{n_i}[W_i]$ -LSS, L' isomorphic to $\bigotimes_{i=1}^T \{P_p^{n_i}[W_i(a_i)]\}$ -LSS, L , by replacing the elements of the characterising matrices by appropriate $n \times n$ matrices and the elements of state input and output by appropriate n -tuples.

We illustrate with example, the procedure for obtaining $\bigotimes_{i=1}^T \{Z_p^{n_i}[W_i]\}$ -LSS, L' isomorphic to $\bigotimes_{i=1}^T \{P_p^{n_i}[W_i(a_i)]\}$ -LSS, L .

Example 3.4.10:

Consider the second order 1-input, 2-output LSS of Example 3.4.1 over the ring $P_2^2[a_1^2+a_1+1] \otimes P_2^2[a_0^2+1]$. The state and output equations of L' are

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} I_4 + W_1 \otimes W_0 & I_2 & W_0 + W_1 \otimes W_0 \\ & I_4 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} I_2 \otimes W_0 \\ W_1 \otimes I_2 \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} I_4 & W_1 \otimes W_0 \\ I_4 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} W_1 \otimes W_0 \\ I_4 \end{bmatrix} u$$

where I_4 is the 4×4 identity matrix.

$W_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ is the companion matrix of $(a_1^2 + a_1 + 1)$ and $W_0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is the companion matrix of $(a_0^2 + 1)$, over $GF(2)$.

In the expanded form the equations are,

$$\begin{bmatrix} x'_{00} \\ x'_{01} \\ x'_{02} \\ x'_{03} \\ x'_{10} \\ x'_{11} \\ x'_{12} \\ x'_{13} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & & & 0 & \\ 0 & 0 & 0 & 0 & & & & \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{02} \\ x_{03} \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{bmatrix}$$

$$\begin{bmatrix} y_{00} \\ y_{01} \\ y_{02} \\ y_{03} \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & & & 0 & \\ 0 & 0 & 0 & 1 & & & & \end{bmatrix} \begin{bmatrix} x_0 \\ x_{01} \\ x_{02} \\ x_{03} \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{bmatrix}$$

where x_{ij} , y_{ij} , $u_i \in GF(2)$. The input sequence elements are 4-tuples and output sequence elements are 8-tuples over $GF(2)$.

L' is a 8th-order LSS over $GF(2)$.

Remark 3.4.1:

We see that in the case of LSS, say, L' over commutative ring of n -tuples, isomorphic to a LSS, say, L and LSS, say L'' , over commutative ring of $n \times n$ matrices, isomorphic to LSS, L , the characterising matrices are identical. The correspondence between the elements of residue class polynomial ring and the $n \times n$ matrices; The procedure to determine these matrices are dealt in Section 2.6.

The procedure for determining the period of the characteristic matrix A of $P_p^n[W]$ -LSS can be used for determining the period of the characteristic matrix \bar{A} of a $Z_p^n[W]$ -LSS isomorphic to $P_p^n[W]$ -LSS. Indeed as shown below the period of A and \bar{A} are same.

Let A be the characteristic matrix of a K th order $P_p^n[W(a)]$ -LSS L . Let \bar{A} denote the characteristic matrix of a $Z_p^n[W]$ -LSS and $L' \simeq L$. As we have seen in this section, \bar{A} is obtained by replacing each element A by appropriate $n \times n$ matrices over $GF(p)$. The size of \bar{A} is hence $nK \times nK$. We show that period of nonsingular matrix A and \bar{A} are same.

Lemma 3.4.1:

A and \bar{A} have same period.

Proof:

Let $\Psi : P_p^n[W(a)] \rightarrow Z_p^n[W]$ be the isomorphism between $P_p^n[W(a)]$ and $Z_p^n[W]$.

$$\text{Let } A = \begin{bmatrix} a_{00} & a_{01} & \dots & a_{0K} \\ \vdots & \vdots & & \vdots \\ a_{K-1,0} & a_{K-1,1} & & a_{K-1,K-1} \end{bmatrix}$$

$$\text{Then } \bar{A} \triangleq \Psi(A) \triangleq \begin{bmatrix} \Psi(a_{00}) & \Psi(a_{01}) & \dots & \Psi(a_{0K}) \\ \vdots & \vdots & & \vdots \\ \Psi(a_{K-1,0}) & \Psi(a_{K-1,1}) & & \Psi(a_{K-1,K-1}) \end{bmatrix}$$

where $a_{ij} \in P_p^n[W(a)]$ and $\Psi(a_{ij}) \triangleq \underline{a}_{ij}$ is an appropriate $n \times n$ matrix over $GF(p)$. Given $a_{ij} \in P_p^n[W(a)]$, the determination of $a_{ij} \in M_p^n[W]$ is discussed in Section 2.6.

Since Ψ is an isomorphism we have

$$\Psi(A^2) = \Psi(A) \cdot \Psi(A) = \bar{A} \cdot \bar{A} = \bar{A}^2$$

Thus $\Psi(A^m) = \bar{A}^m$ m , any integer.

Hence if T is the period of A , it is the least integer such that

$$\Psi(A^T) = \Psi(I_{K \times K}) = \bar{A}^T = I_{nK \times nK}$$

Thus if A and \bar{A} have one to one correspondence, period of \bar{A} is also equal to T .

\bar{A} is of size $K \times K$ over the ring $Z_p^n[W]$ or $M_p^n[W]$.

Computations of period of \bar{A} over $GF(2)$, can be done in terms of period of A .

Example 3.4.11:

Consider the characteristic matrix $A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ over $P_2^{16}[a^{16}+1]$ of Example 3.3.11.

$$\text{Here } \bar{A} = \begin{bmatrix} \underline{0} & \underline{I} \\ \underline{a} & \underline{a} \end{bmatrix}$$

where $\underline{0}$ is a 16×16 null matrix

\underline{I} is a 16×16 identity matrix

and \underline{a} is a 16×16 cyclic matrix

$$\underline{a} = \begin{bmatrix} 0 & 0 & \dots & 1 \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \in M_2^{16}[W]$$

A and \bar{A} have one-to-one correspondence.

Hence the period of 32×32 matrix \bar{A} over $GF(2)$ is equal to the period of 2×2 matrix A over $P_2^{16}[a^{16}+1]$ which is 48, as computed in Example 3.3.11.

Example 3.4.12:

Consider the characteristic matrix $A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ over $P_2^3[(a+1)^3]$, $(a+1)^3 = a^3 + a^2 + a + 1$.

Here $\bar{A} = \begin{bmatrix} \underline{0} & \underline{I} \\ \underline{a} & \underline{a} \end{bmatrix}$

where $\underline{0}$ is a null matrix of size 3×3

\underline{I} is an identity matrix of size 3×3

and $\underline{a} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

A and \bar{A} have one-to-one correspondence. Hence, period of \bar{A} is equal to the period of A , and is equal to 12.

Example 3.4.13:

Consider $A = \begin{bmatrix} a^2 & 1+a \\ 1+a+a^2 & a \end{bmatrix}$ over $P_2^3[a^3+1]$ of Examples 3.3.12 and 3.3.14. The period of A is 6 as computed in Examples 3.3.12 and 3.3.14.

$$\bar{A} = \begin{bmatrix} \underline{a^2} & \underline{1+a} \\ \underline{1+a+a^2} & \underline{a} \end{bmatrix}$$

Over $GF(2)$ \bar{A} is

$$\bar{A} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

A and \bar{A} have one to one correspondence. Hence the period of \bar{A} is 6.

Example 3.4.14:

Consider $A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ over $P_2^{10}[a^{10}+1]$ of Example 3.3.16.

Period of A is computed as 510.

$$\bar{A} = \begin{bmatrix} \underline{0} & \underline{I} \\ \underline{a} & \underline{a} \end{bmatrix}$$

$\underline{0}$, \underline{I} are of size 10×10

\underline{a} is a 10×10 cyclic matrix

$$\text{Over } GF(2) \bar{A} = \begin{bmatrix} \underline{0} & \underline{I} \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

A and \bar{A} have one-to-one correspondence. Hence period of $\bar{A} = 510$.

Example 3.4.15:

Consider $A = \begin{bmatrix} (1+a) & 1 \\ a & a \end{bmatrix}$ over $P_2^6[(a^3+a^2+1)(a^3+a+1)]$
of Example 3.3.13. Period of A is 63.

$$\bar{A} = \begin{bmatrix} \underline{(1+a)} & \underline{1} \\ \underline{a} & \underline{a} \end{bmatrix}$$

$$(a^3+a^2+1)(a^3+a+1) = (a^6+a^5+a^4+a^3+a^2+a+1)$$

\bar{A} over $GF(2)$ is

$$\bar{A} = \left[\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right]$$

A and \bar{A} have one-to-one correspondence. Hence period of \bar{A} is 63.

Remark 3.4.2:

Since the order of $Z_p^n[W]$ or $\bigotimes_{i=1}^r Z_p^{n_i}[W_i]$ is same as

the order of $P_p^n[W(a)]$ or $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ respectively, unlike the case of $M_p^n[W]$ -LSS or $\bigotimes^T \{M_p^n[W_i]\}$ -LSS, $Z_p^n[W]$ -LSS or $\bigotimes^T \{Z_p^{n_i}[W_i]\}$ -LSS can handle all possible n -tuples over $GF(p)$.

In the next section we deal with the implementation over $GF(p)$ of $Z_p^n[W]$ -LSS isomorphic to $P_p^n[W(a)]$ -LSS and $\bigotimes^T \{Z_p^{n_i}[W_i]\}$ -LSS isomorphic to $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ -LSS.

3.5 IMPLEMENTATION OF LSS OVER RING OF n -TUPLES ISOMORPHIC TO THE LSS OVER RESIDUE CLASS POLYNOMIAL RINGS:

In this section implementation of LSS over ring of n -tuples, isomorphic to $P_p^n[W(a)]$ -LSS and $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ -LSS discussed in Sections 3.1 and 3.4 respectively are taken up. We have seen in Section 2.6, that ring of n -tuples $Z_p^n[W]$ and $\bigotimes^T \{Z_p^{n_i}[W_i]\}$ can be obtained which are isomorphic to $P_p^n[W(a)]$ and $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$. The addition operation in the ring of n -tuples is pointwise modulo p , whereas the multiplication operation is appropriate matrix and vector multiplication modulo p . If the elements of state input and output are n -tuples over $GF(p)$, as the multiplication operation of two n -tuples is matrix and vector multiplication, the elements of the characterising matrices will then become appropriate $n \times n$ matrices. This enables us to implement $Z_p^n[W]$ -LSS and $\bigotimes^T \{Z_p^{n_i}[W_i]\}$ -LSS isomorphic to $P_p^n[W(a)]$ -LSS and $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ -LSS respectively. Thus a LSS L over the residue class polynomial

ring is reduced to a LSS L' over $GF(p)$. If the $n \times n$ submatrices of the characterising matrices and n -tuples of state, input and output of L' are treated as a single unit, the order of L' is K . On the other hand if the elements are treated to be from $GF(p)$, the order of L' is nK . The set of all such LSS isomorphic to LSS over residue class polynomial rings constitute a subclass of $GF(p)$ -LSS of order nK .

3.5.1 Implementation of LSS over $Z_p^n[W]$, $Z_p^n[W]$ -LSS:

In what follows we consider $Z_p^n[W]$ -LSS isomorphic to $P_p^n[W(a)]$ -LSS, which can be studied in terms of lower order $P_p^n[W(a)]$ -LSS. A single input single output K th order LSS, say, L over $P_p^n[W(a)]$ is first considered. The schematic diagram is given in Figure 3.5.1. The discussion holds good for implementation of L' over $\bigotimes_{i=1}^T \{Z_p^{n_i}[W_i]\}$ -LSS $\simeq \bigotimes_{i=1}^T \{P_p^{n_i}[W_i(a_i)]\}$ -LSS.

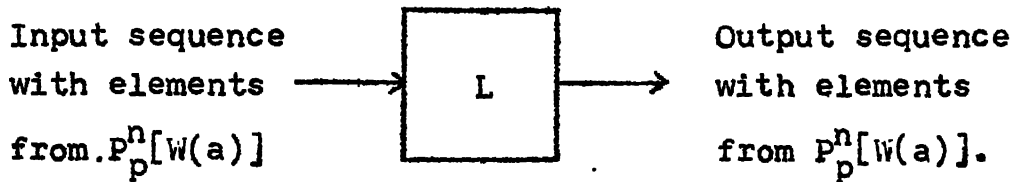


Figure 3.5.1: A single input single output LSS over $P_p^n[W(a)]$.

L is defined by the state and output equations (3.1.3) and (3.1.4) which are rewritten here

$$x(N+1) = A x(N) + B u(N)$$

$$y(N) = C x(N) + D u(N)$$

The elements of state $x(N)$, characterising matrices A, B, C and D and the sequence $u(N)$ of input and $y(N)$ of output are from residue class polynomial ring.

The computation of $x(N+1)$ involves the multiplication of elements of A and $x(N)$, B and $u(N)$ and their addition. Similarly in the computation of $y(N)$ multiplication of elements of C and $x(N)$, D and $u(N)$ and their addition are involved. As already stated, in $Z_p^n[W] \simeq P_p^n[W(a)]$, the addition of two elements is pointwise modulo p addition, whereas the multiplication is multiplication of $n \times n$ matrix corresponding to one n -tuple and $n \times 1$ vector corresponding to the other n -tuple.

Thus if we replace the elements of the characterising matrices by the corresponding $n \times n$ matrices over $GF(p)$ and the elements of state sequence $\{x(N)\}$, input sequence $\{u(N)\}$ and output sequence $\{y(N)\}$ by n -tuples we get state and output equations over $GF(p)$ which correspond to a n -input n -output LSS say L' over $GF(p)$. Thus L' is capable of processing n -tuples over $GF(p)$. The order of L' is nK .

We can view that LSS L is implemented as L' over $GF(p)$. They are actually two different systems which are isomorphic.

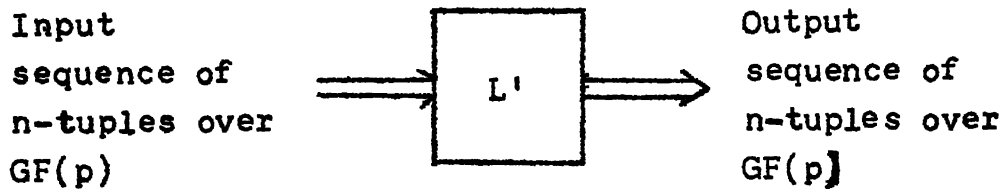


Figure 3.5.2: A n -input n -output system over $GF(p)$

If we have such a system L' of order nK , the analysis of L of order K , isomorphic to L' of order nK is less complex. The results of analysis of L can then be interpreted in terms of analysis of L' over $GF(p)$.

Now we take up a general case.

Consider a K th order m -input, j -output $P_p^n[W(a)]$ -LSS say L . Let the state and output equations be as given by Equations (3.1.3) and (3.1.4). As in the single input single output case, if we replace the elements of the characterising matrices by the corresponding $n \times n$ matrices over $GF(p)$ from $M_p^n[W]$ and the elements of x, u and y by n -tuples, we get state and output equations over $GF(p)$, which correspond to a LSS, say L' over $GF(p)$. Then L' is a mn -input and jn -output system whose order is nK .

We can view that, LSS L is implemented as L' over $GF(p)$. They are two isomorphic systems. In L' each element is treated as n -tuple. The schematic diagram is given in Figures 3.5.3a and 3.5.3b.

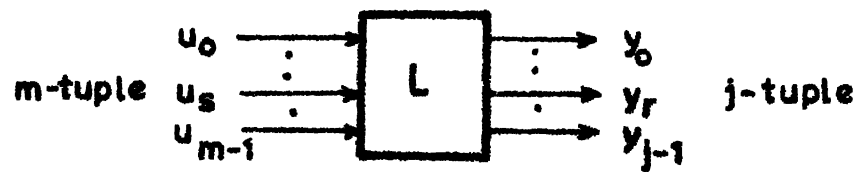


Fig. 3.5.3 a LSS over $P_p^n [W(a)]$

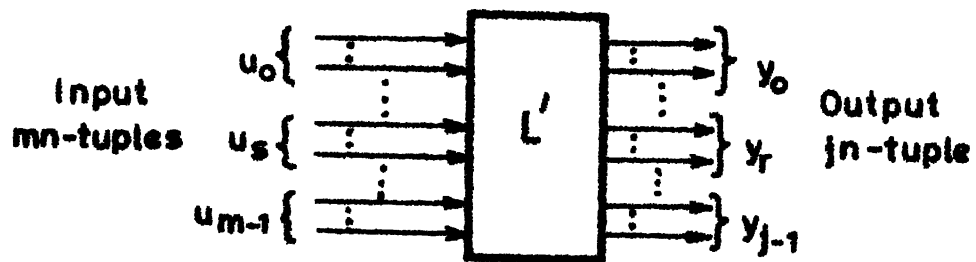


Fig. 3.5.3b LSS over $Z_p^n \cong P_p^n [W(a)]$

Given a LSS, say L , over $P_p^n[W(a)]$, We next consider the implementations of L' over $Z_p^n[W] \simeq P_p^n[W(a)]$.

Every line in L is replaced by a bundle of n lines. Each adder in $P_p^n[W(a)]$ is replaced by n adders over $GF(p)$. Multiplication by a constant in $P_p^n[W(a)]$ corresponds to matrix and vector multiplication in Z_p^n . Hence each coefficient multiplier in $P_p^n[W(a)]$, is replaced by an array of coefficient multipliers and adders in $GF(p)$. Each delay element in $P_p^n[W(a)]$ is replaced by a bank of n delay elements in $GF(p)$.

If a line in L carries a value $q(a) = \sum_{i=0}^{n-1} q_i a^i \in P_p^n[W(a)]$, the corresponding n lines in L' carry a vector value

$$q = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{bmatrix}$$

The equivalence between the adders multipliers and delayers in L and L' are given in Figure 3.5.4.

Likewise the basic component L and L' over $\bigotimes_{i=1}^T \{P_p^{n_i}[W_i(a_i)]\}$ and $\bigotimes_{i=1}^T \{Z_p^{n_i}[W_i]\}$ can be obtained.

The procedure for obtaining Z_p^n -LSS, $L' \simeq P_p^n[W(a)]$ -LSS, L is outlined in the following example.

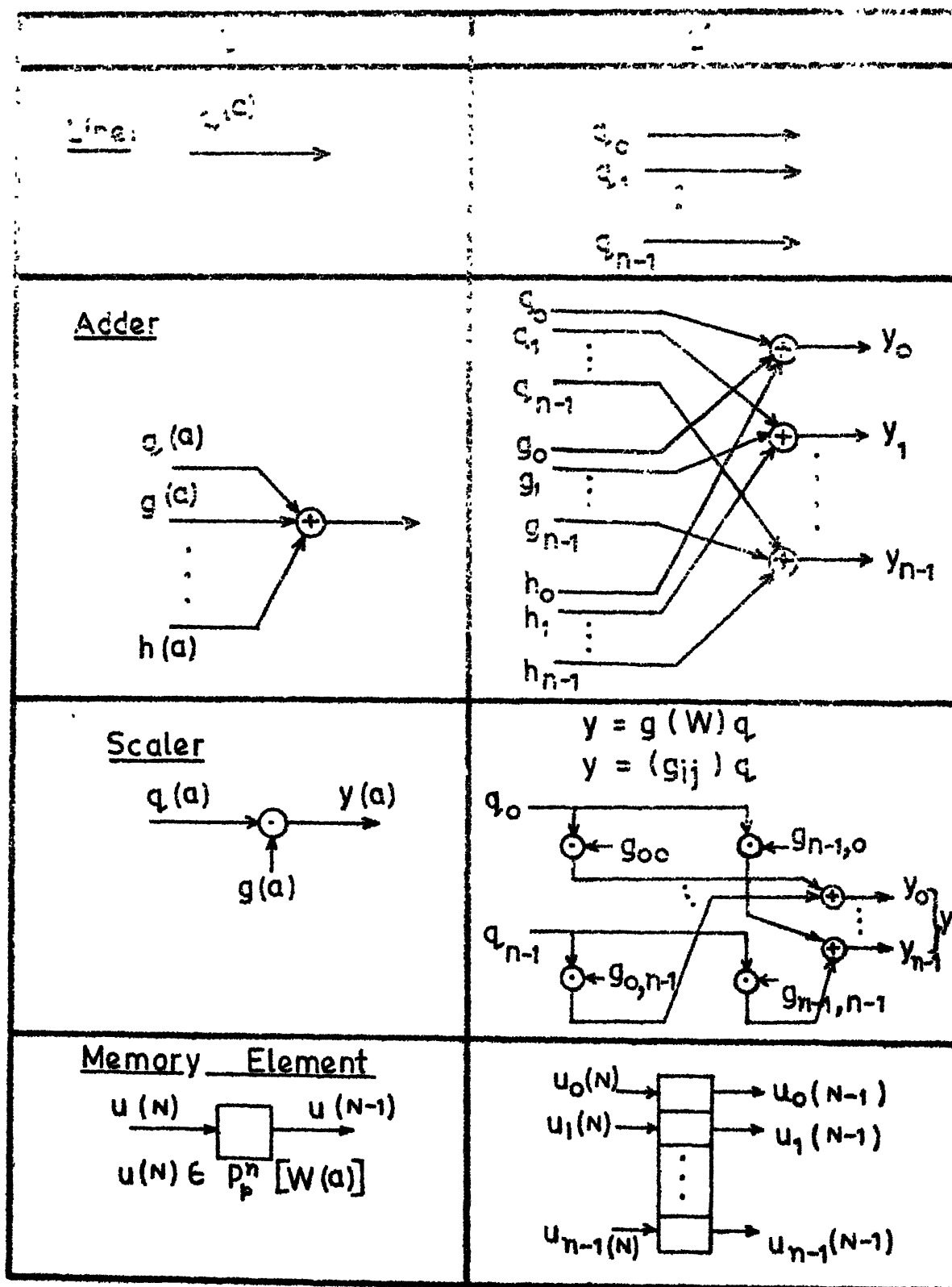


Fig.3.5.4 Basic Components of L and L'

Example 3.5.1:

Consider the second order 1-input, 2-output-LSS over $P_2^2[(a^2+1)]$ of Example 3.4.7 whose characterising matrices are

$$A = \begin{bmatrix} 1+a & a \\ 1 & 0 \end{bmatrix}; \quad B = \begin{bmatrix} a \\ 1 \end{bmatrix}; \quad C = \begin{bmatrix} 1 & a \\ 1 & 0 \end{bmatrix}; \quad D = \begin{bmatrix} 0 \\ a \end{bmatrix}$$

The schematic diagram of LSS L over $P_2^2[a^2+1]$ is given in Figure 3.5.5a.

The LSS L' over $Z_2^2[W] \simeq P_2^2[a^2+1]$ has the corresponding characterising matrices,

$$A' = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}; \quad B' = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}; \quad C = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}; \quad D' = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$$

as given in Example 3.4.7.

The schematic diagram of LSS, is given in Figure 3.5.5b.

3.5.2 Implementation of LSS Over $\bigotimes_{i=0}^{r-1} \{Z_p^{n_i}[W_i]\}$, $\bigotimes_{i=0}^{r-1} \{Z_p^{n_i}[W_i]\}$ -LSS:

The implementation of $\bigotimes_{i=0}^{r-1} \{Z_p^{n_i}[W_i]\}$ -LSS is carried out on lines similar to the implementation of $Z_p^n[W]$ -LSS. Given a LSS, say, L over $\bigotimes_{i=0}^{r-1} \{P_p^{n_i}[W_i(a_i)]\}$ where $\sum_{i=0}^{r-1} n_i = n$, we

consider below the implementation of L' over $\bigotimes_{i=0}^{r-1} \{Z_p^{n_i}[W_i]\}$

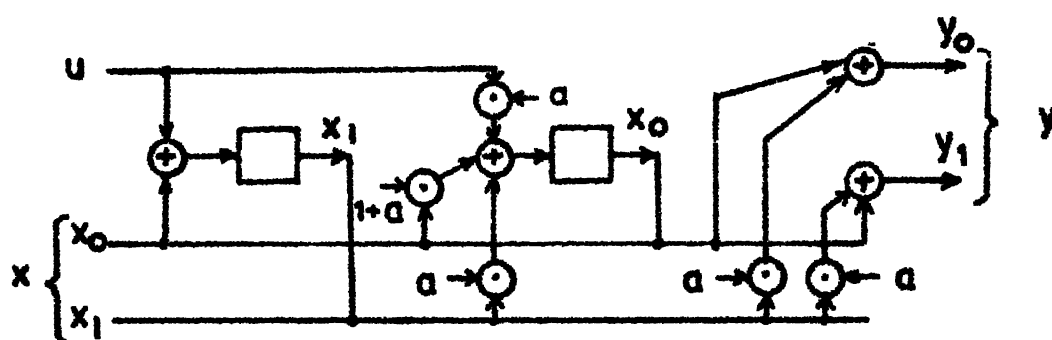


Fig. 3.5.5a $P_2^2[a^2+1]$ -LSS, L of Example 3.5.1

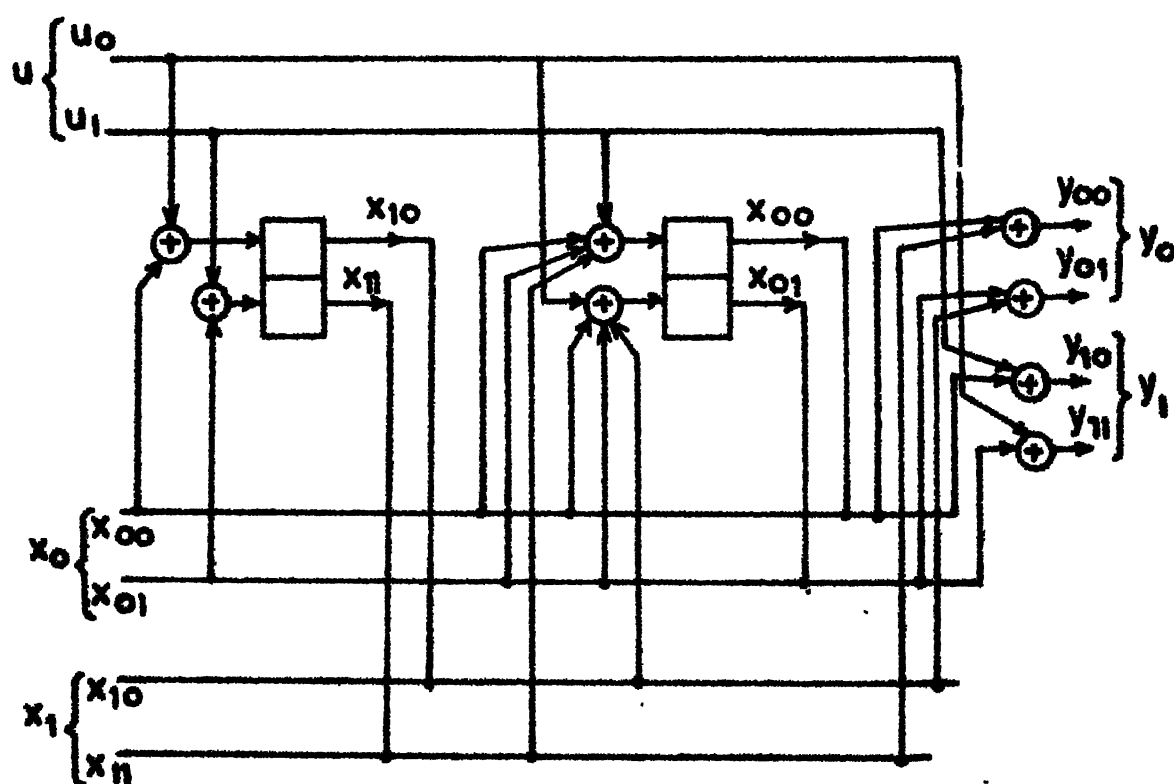


Fig. 3.5.5b $Z_2^2[W]$ -LSS $\cong P_2^2[a^2+1]$ -LSS, L' of Example 3.5.1

isomorphic to $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$. Every line in L is replaced by a bundle of n lines. Each adder in $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ is replaced by n adders over $GF(p)$. Multiplication by a constant in $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ corresponds to matrix and vector multiplication in $\bigotimes^T \{Z_p^{n_i}[W_i]\}$. Hence each coefficient multiplier in $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ is replaced by an array of coefficient multipliers and adders in $GF(p)$. Each delay element in $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ is replaced by a bank of n delay elements in $GF(p)$.

If a line in L carries a value

$$q(a_{r-1}, a_{r-2}, \dots, a_1, a_0) = \sum_{i_{r-1}=0}^{n_{r-1}-1} \dots \sum_{i_0=0}^{n_0-1} q_{i_{r-1}, i_{r-2}, \dots, i_1, i_0}$$

$$a_{r-1}^{i_{r-1}} a_{r-2}^{i_{r-2}} \dots a_1^{i_1} a_0^{i_0}$$

in $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ the corresponding n lines in L' carry a vector value

$$q = \begin{bmatrix} q_{00\dots 0} \\ q_{00\dots 1} \\ \vdots \\ q_{i_{r-1}i_{r-2}\dots i_1i_0} \\ \vdots \\ q_{n_{r-1}-1, n_{r-2}-1, \dots, n_0-1} \end{bmatrix}$$

The equivalence between the adders multipliers and delayers in L and L' can be obtained in a manner similar to the case of $P_p^n[W(a)]$ -LSS.

Example 3.5.2:

Consider LSS of order one, over $P_2^2[a_1^2+1] \otimes P_2^2[a_0^2+a_0+1]$
Let $A = [1+a_1a_0]$, $B=[a_1a_0]$, $C=[a_1]$; $D=[a_0]$.

In this example $W_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$; $W_0 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$;

$$a_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}; \quad \text{we have } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$a_0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix};$$

$$(1+a_1a_0) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

The LSS over $P_2^2[a_1^2+1] \otimes P_2^2[a_0^2+a_0+1]$ and $Z_2^2[W_1] \otimes Z_2^2[W_0]$ are given in Figure 3.5.6a and 3.5.6b respectively.

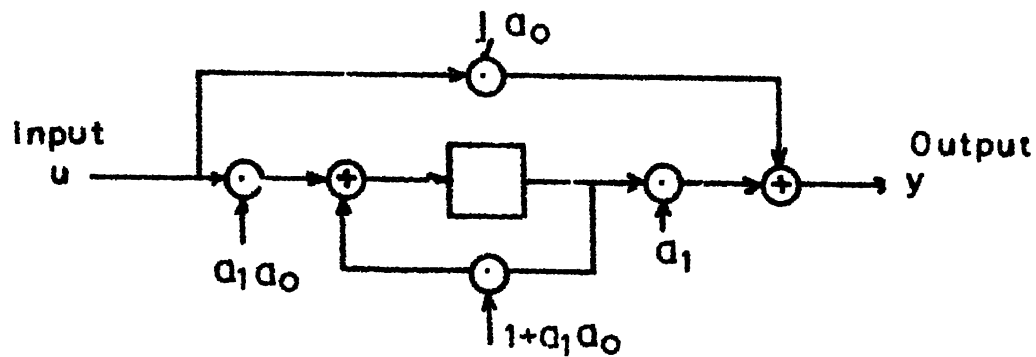


Fig. 3.5.6a $P_2^2 [a_1^2 + 1] \otimes P_2^2 [a_0^2 + a_0 + 1] - \text{LSS}$
of Example 3.5.2

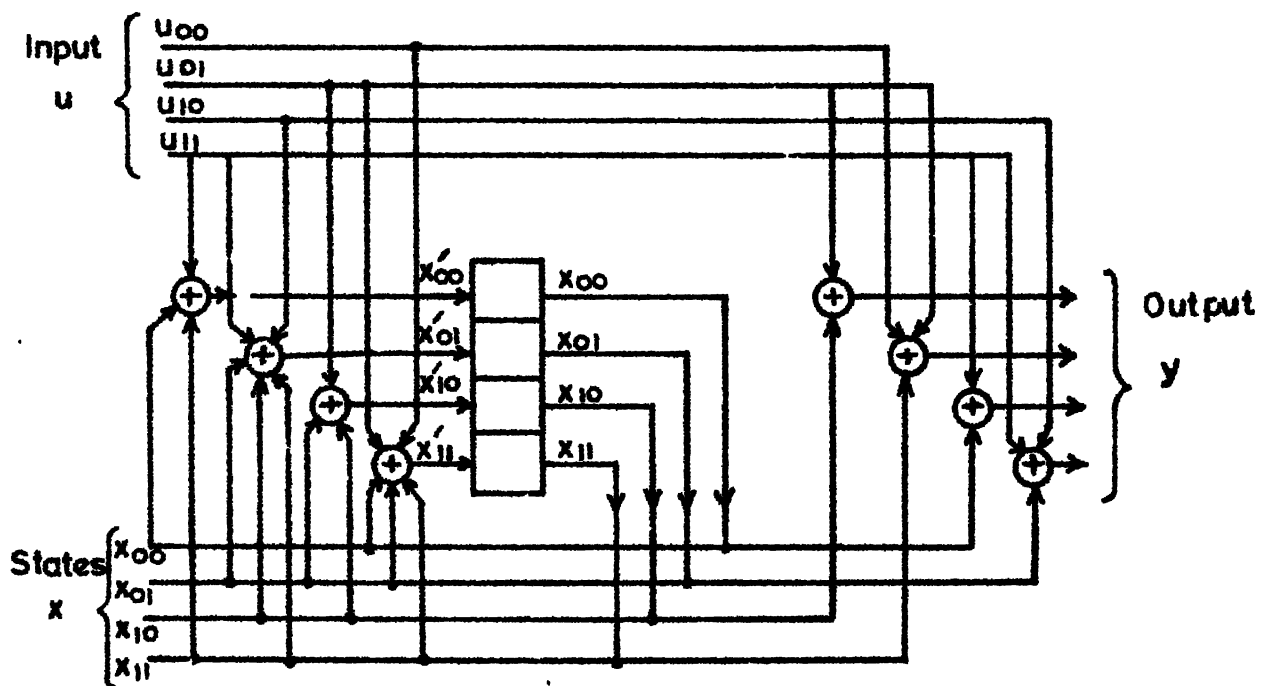


Fig.3.5.6b $Z_2^2 [W_1] \otimes Z_2^2 [W_0] - \text{LSS}$ of Example 3.5.2

3.5.3 Implementation of $Z_p^n[W]$ -LSS Isomorphic to $P_p^n[a^n-1]$ -LSS with Serial Multiplication:

We have seen in Section 2.6 that the rings of n -tuples over $GF(p)$, are isomorphic to residue class polynomial rings. The addition of n tuples are pointwise modulo p addition and multiplication operation is appropriate matrix-vector multiplication. We show now that when the residue class polynomial ring is $P_p^n[a^n-1]$, the multiplication of two n -tuples (from Z_p^n) corresponding to any two elements, say, $g(a)$ and $q(a)$ from $P_p^n[a^n-1]$, becomes multiplication of an appropriately chosen $n \times n$ cyclic matrix corresponding to $g(a)$ and an $n \times 1$ vector corresponding to $q(a)$ over $GF(p)$. The multiplication operation with serial implementation results in a simpler hardware structure.

Let the two elements $g(a), q(a) \in P_p^n[a^n-1]$ be $g(a) = g_0 + g_1a + g_2a^2 + \dots + g_{n-1}a^{n-1}$ and $q(a) = q_0 + q_1a + \dots + q_{n-1}a^{n-1}$. Consider their product $y(a) = g(a)q(a)$.

The companion matrix of (a^n-1) is

$$W = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}$$

As discussed in Section 2.6

$$y = \left[\sum_{i=0}^{n-1} g_i W^i \right] \cdot q$$

$$= \begin{bmatrix} g_0 & g_{n-1} & \cdots & g_2 & g_1 \\ g_1 & g_0 & & g_3 & g_2 \\ \vdots & \vdots & & \vdots & \vdots \\ g_{n-2} & g_{n-3} & & g_0 & g_{n-1} \\ g_{n-1} & g_{n-2} & & g_1 & g_0 \end{bmatrix} \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-2} \\ q_{n-1} \end{bmatrix} \quad (3.5.1)$$

In general we need n^2 multipliers and n modulo p adders to perform this multiplication in one clock cycle. We note that in Equation (3.5.1) the matrix is cyclic. This facilitates simple serial implementation over $GF(p)$ using cyclic shift registers, as shown in Figure 3.5.7. The corresponding output is $g_0 q_0 + g_{n-1} q_1 + \cdots + g_2 q_{n-2} + g_1 q_{n-1}$ which is the constant term in the product $y(a)$. After a cyclic shift of one position the output is

$g_0 q_1 + g_{n-1} q_2 + \cdots + g_2 q_{n-1} + g_1 q_0$ which is equal to the coefficient y_1 in $y(a)$. Similarly at the j th cyclic shift $0 \leq j \leq n-1$, the output is

$$y_j = \sum_{m=0}^{n-1} g_m q_{j \ominus m} \quad (3.5.2)$$

where \ominus is the subtraction modulo n operation.

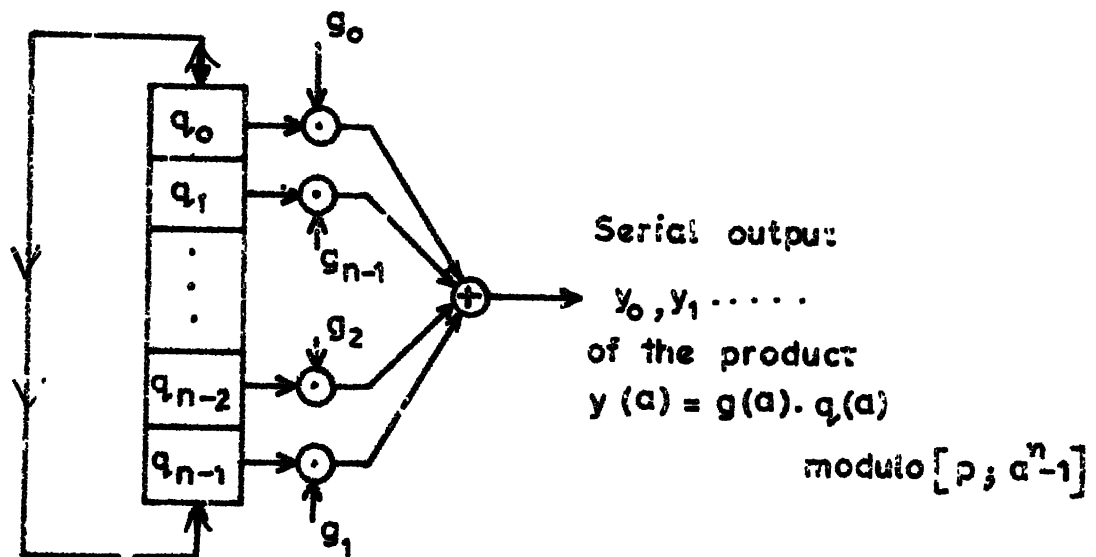


Fig. 3.5.7 Serial implementation of multiplications
 in $\mathbb{Z}_p^n \cong \mathbb{P}_p^n[a^n - 1]$

Thus the serial output is y_0, y_1, \dots, y_{n-1} .

For serial multiplication, only n multipliers and one modulo p adder are needed.

If the multiplication is done by a fixed element $g(a)$, then in the Figure 3.5.7 the scalars g_0, g_1, \dots, g_{n-1} are the coefficients of $g(a)$. The variable element $q \approx q(a)$ is stored in the cyclic shift register.

An example of system with bit serial operation is given in Example 3.5.3.

The application of serial operation in encoding will be discussed in Section 5.5.

Example 3.5.3:

Consider the elements $q(a) = (1+a+a^3)$ and $g(a) = (1+a^2+a^3)$ in the residue class polynomial ring $P_2^4[a^4+1]$.

We have $q(a) = (1+a+a^3) \approx \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$ which is stored in the cyclic shift register. We implement serial multiplication using cyclic shift register. With reference to Figure 3.5.8 we have with $g_0=1, g_1=0, g_2=g_3=1$, output $= [0001]^{t_r} \approx a^3$.

Example 3.5.4:

Consider the elements $q(a) = (1+2a+2a^2)$ and $g(a) = (2+2a+a^2)$ in the ring $P_3^3[a^3-1]$. We have $q(a) = \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}$ which is

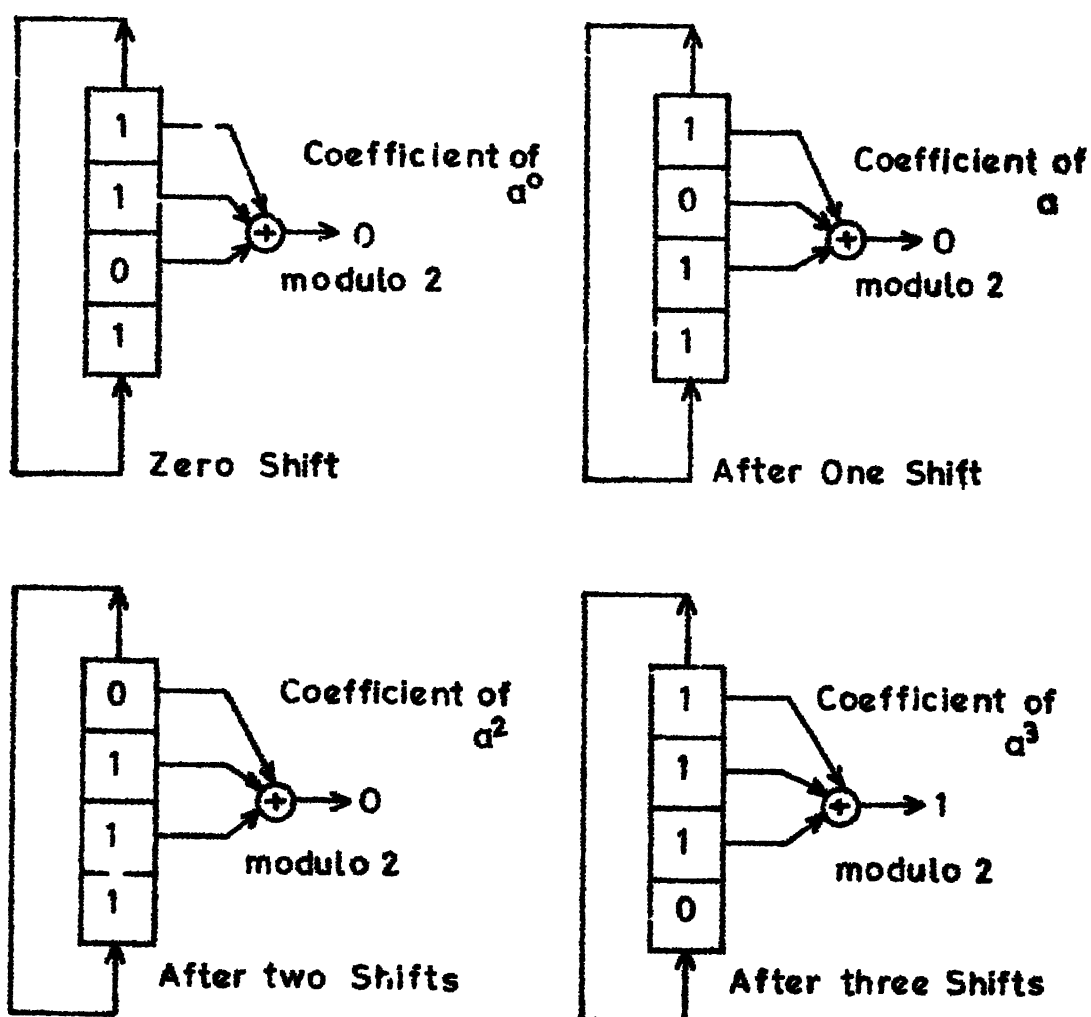


Fig.3.5.8 Output of the Serial Multiplier After Successive Cyclic Shifts

stored in the cyclic shift register. With reference to Figure 3.5.9 we have with $g_0=2$, $g_1=2$, $g_2=1$, the output

$$\text{is } \begin{bmatrix} 2 \\ 2 \\ 0 \end{bmatrix} \neq 2+2a.$$

Before concluding the section we give some more examples of LSS.

Example 3.5.5:

Consider a second order zero input $P_2^n[a^n+1]$ -LSS as shown in Figure 3.5.10.

The state and output equations of this system are

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}$$

$$y = [1 \quad 0] \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}$$

where all the entries $\in P_2^n[a^n+1]$.

Consider the implementation of Z_2^n -LSS $\simeq P_2^n[a^n+1]$ -LSS as in Figure 3.5.11 where No. 0 and No. 1 indicate the stage number and 0,1,2,...n-1 in each stage indicate the number of the memory element.

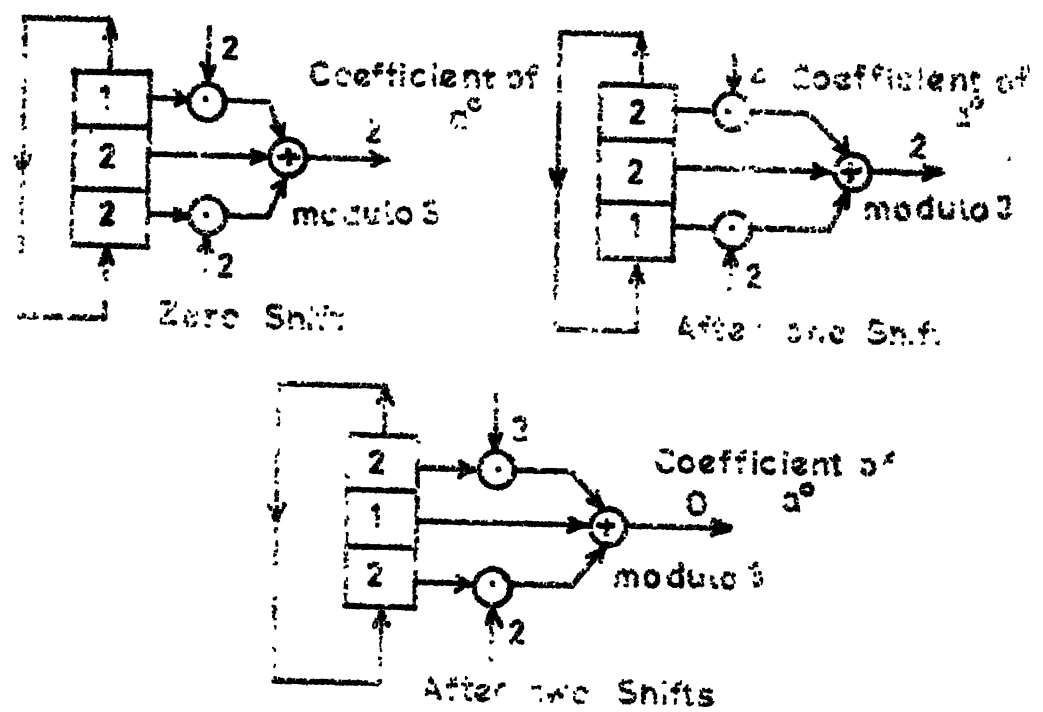


Fig.3.5.8 Output of the Serial Multiplier
After successive Cyclic Shifts

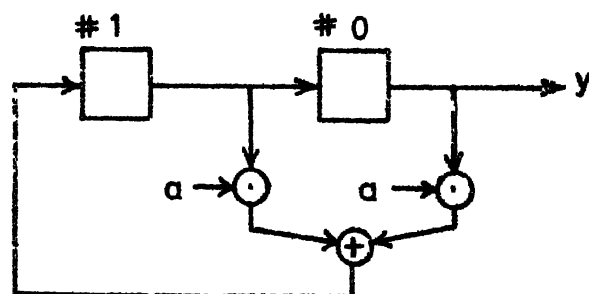


Fig.3.5.10 $P_2^2[a^n-1]$ -LSS of Example 3.5.5

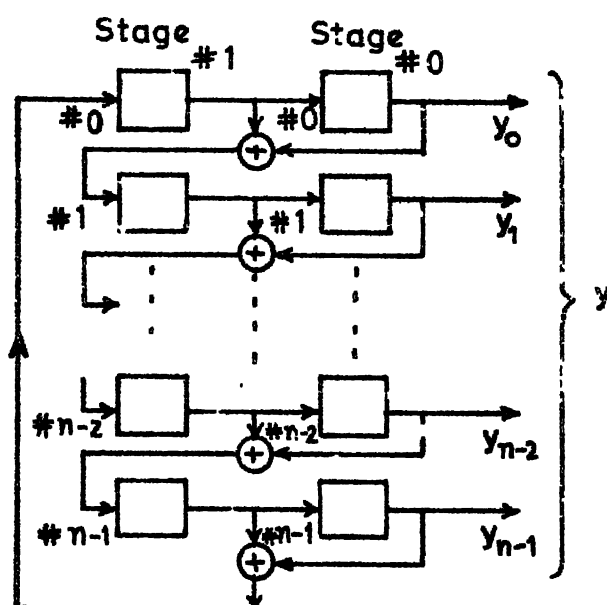


Fig.3.5.11 $Z_2^n[W]$ -LSS of Example 3.5.5

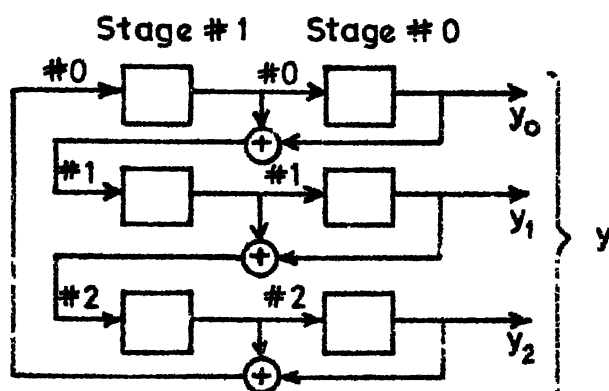


Fig.3.5.12 $Z_2^3[W]$ -LSS of Example 3.5.5

The state and output equations of this system are

$$\begin{bmatrix} x'_{00} \\ x'_{01} \\ \vdots \\ x'_{0,n-1} \\ x'_{10} \\ x'_{11} \\ \vdots \\ x'_{1n-1} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ \vdots \\ x_{0n-1} \\ x_{10} \\ x_{11} \\ \vdots \\ x_{1n-1} \end{bmatrix}$$

and

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ \vdots \\ x_{0n-1} \\ x_{10} \\ x_{11} \\ \vdots \\ x_{1n-1} \end{bmatrix}$$

where all the entries $\in \text{GF}(2)$.

This is the random number generator proposed by Radar, Rabiner and Schafer [52], but is not looked from the point of view of $Z_2^n[W]$ -LSS. The initial state used in the

reference is $\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, $\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$. The output is a sequence of n -tuples which are converted to decimal numbers. The output n -tuple $[y_0, y_1, \dots, y_{n-1}]$ is a column vector of coefficients of corresponding element $y(a \text{ polynomial}) \in P_2^n[a^n+1]$.

For $n=3$ the implementation of Z_2^3 -LSS $\simeq P_2^3[a^3+1]$ -LSS is as given in Figure 3.5.12 where No. 1 and No. 0 indicate the stage number and 0,1,2 in each stage indicate the number of the memory element.

The state and output equations are

$$\begin{bmatrix} x'_{00} \\ x'_{01} \\ x'_{02} \\ x'_{10} \\ x'_{11} \\ x'_{12} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{02} \\ x_{10} \\ x_{11} \\ x_{12} \end{bmatrix}$$

and

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{02} \\ x_{10} \\ x_{11} \\ x_{12} \end{bmatrix}$$

We have seen that when the residue class polynomial ring is $P_p^n[a^n-1]$, multiplication of ring elements in $Z_p^n[W] \simeq P_p^n[a^n-1]$ can be carried out serially by using cyclic shift registers. Based on this principle, in the next example we give an alternative implementation of the random number generator considered in Example 3.5.5. We shall see that this implementation requires only one modulo-2 adder instead of n modulo-2 adders. However the implementation, being serial, is slow and requires an additional n bit storage shift register.

Example 3.5.6:

Consider the $P_2^n[a^n-1]$ -LSS of Example 3.5.5. Its serial implementation is given in Figure 3.5.13.

The system requires two clocks: a faster shift clock for shifting the contents of n bit storage shift register and the two cyclic shift registers, and a slower transfer clock for transferring the contents of the n bit storage shift register and the two cyclic shift registers. The initial state is $x(o) = \begin{bmatrix} x_o(o) \\ x_1(o) \end{bmatrix}$.

where $x_o(o) = [x_{o,0}(o), x_{o,1}(o), \dots, x_{o,(n-1)}(o)]^T = [1, 0, \dots, 0]^T$
and $x_1(o) = [x_{1,0}(o), x_{1,1}(o), \dots, x_{1,(n-1)}(o)]^T = [0, 0, \dots, 0]^T$

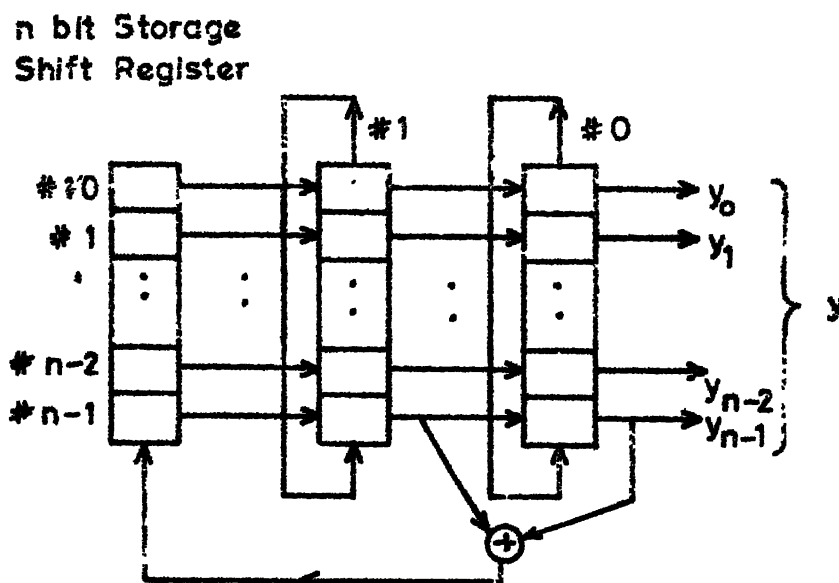


Fig. 3.5.13 Serial Implementation of $Z_2^n[W]$ -LSS
of Example 3.5.6

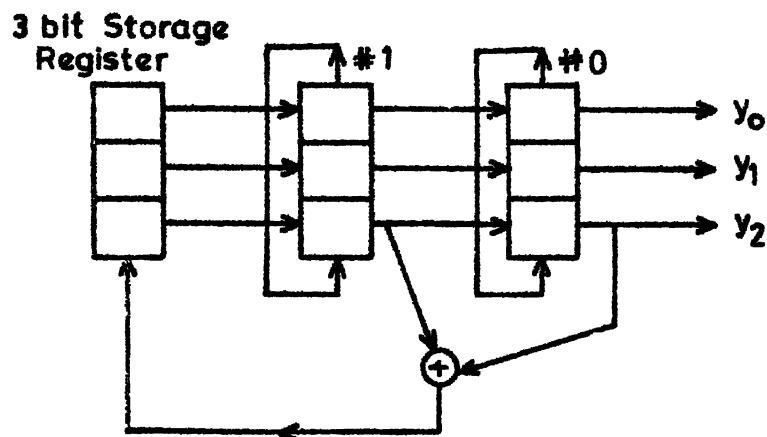


Fig. 3.5.14 Serial Implementation of $Z_2^3[W]$ -LSS
of Example 3.5.6

At the zeroth instant the zeroth bit $x_{1,0}(1)$ of $x_1(1)$ is computed, as

$$x_{1,0}(1) = x_{0,(n-1)}(0) \oplus x_{1,(n-1)}(0).$$

and at the first shift clock pulse is stored in the storage register at location $(n-1)$. Then the contents of the cyclic shift register No. 0 and No. 1 are cyclic shifted.

At the 2nd shift clock pulse the 1st bit, $x_{00}(0) \oplus x_{10}(0)$, of $x_1(1)$ is computed and stored in the storage shift register at location $(n-1)$ and its previous content is shifted to location $n-2$. Thus during the n shift clock pulses, the bits of $x_1(1)$ are computed after each cyclic shift and are stored in the storage register. Before the $(n+1)$ th shift clock pulse, by means of transfer clock pulse, the contents of storage register is transferred to stage No. 1 and contents of stage No. 1 is transferred to stage No. 0. The output n -tuple $(y_0, y_1, \dots, y_{n-1})$ is converted to decimal.

For $n=3$ the serial implementation of the above system is given in Figure 3.5.14. At the first shift clock pulse, at location 2 of the 3 bit storage register, the zeroth bit of $x_1(1)$, i.e. $x_{10}(1) = x_{12}(0) \oplus x_{02}(0)$ is stored and simultaneously the contents of cyclic shift registers No. 1 and No. 0 are cyclically shifted.

At the second shift clock pulse, the contents of location 2 of the 3 bit storage register $x_{10}(1)$ is shifted to location 1 and the $x_{11}(1) = x_{10}(0) \oplus x_{00}(0)$ is stored in location 2. The contents of cyclic shift registers No. 1 and No. 0 are cyclically shifted. At the 3rd shift clock pulse, content of location 1 of the 3 bit storage register $x_{10}(1)$ is shifted to location 0, content of location 2 $x_{11}(1)$ is shifted to location 1 and $x_{12}(1) = x_{11}(0) \oplus x_{01}(0)$ is stored in location 2 of 3 bit storage register. The contents of cyclic shift registers are cyclically shifted. Now the cyclic shift register contents are equal to the contents to start with; No. 1 has $x_1(0)$, No. 0 has $x_0(0)$. The contents of storage register is the computed value $x_1(1)$. Before the next shift clock pulse is applied, the transfer clock pulse transfers the contents of storage register to cyclic shift register No. 1 and contents of cyclic shift register No. 1 to cyclic shift register No. 0. The output bit. (y_0, y_1, y_2) are converted to decimal.

Example 3.5.7:

Consider the fourth-order $P_2^2[a^2+a+1]$ -LSS as shown in Figure 3.5.15a.

The state and output equations of this system are

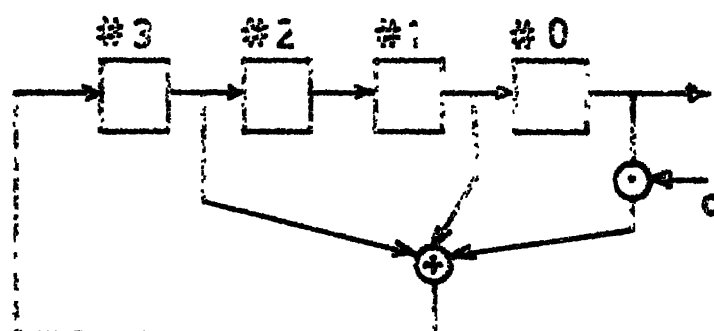


Fig. 3.5.15a $P_2^2[a^2+a+1]$ -LSS of Example 3.5.7

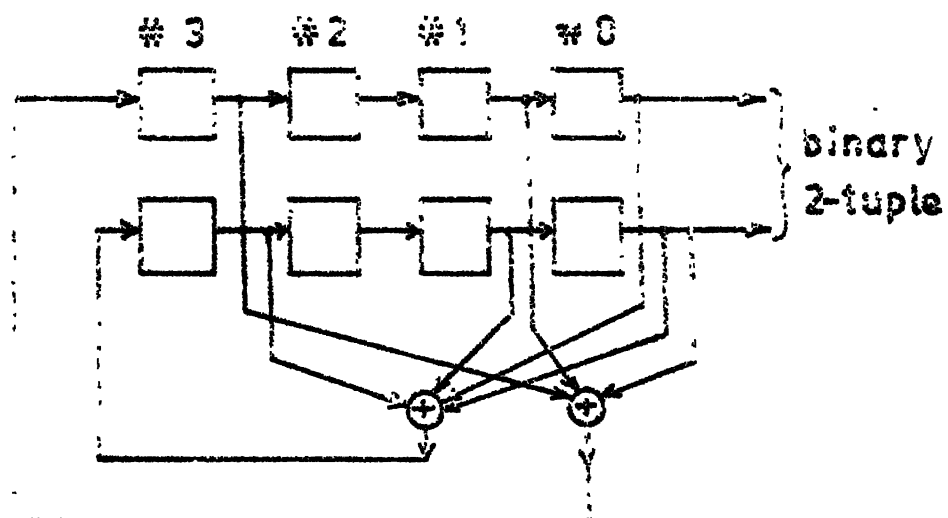


Fig. 3.5.15b $Z_2^2[W]$ -LSS of Example 3.5.7

$$\begin{bmatrix} x'_0 \\ x'_1 \\ x'_2 \\ x'_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$$y = [1 \ 0 \ 0 \ 0] \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

where all the entries $\in P_2^2[a^2+a+1]$. The $Z_2^2[w]$ -LSS, L' isomorphic to L is given in Figure 3.5.15b.

The state and output equations of L' are

$$\begin{bmatrix} x'_{00} \\ x'_{01} \\ x'_{10} \\ x'_{11} \\ x'_{20} \\ x'_{21} \\ x'_{30} \\ x'_{31} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{10} \\ x_{11} \\ x_{20} \\ x_{21} \\ x_{30} \\ x_{31} \end{bmatrix}$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{10} \\ x_{11} \\ x_{20} \\ x_{21} \\ x_{30} \\ x_{31} \end{bmatrix}$$

L' is the maximum length sequence generator over $GF(2^2)$ with binary 2-tuple as output.

The scheme of Figure 3.5.15b is an example of $Z_2^2[W]$ -LSS $\simeq P_2^2[a^2+a+1]$ -LSS, proposed in [23,24], though not looked from the point of view of a LSS over $P_2^2[a^2+a+1]$, for the generation of 4-level pseudorandom sequence obtained by linearly combining the output binary 2-tuples.

Example 3.5.8:

Consider the second-order $P_2^2[a^2+a+1]$ -LSS, L as given in Figure 3.5.16a.

The system is described by the following equations

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u$$

$$y = [a \quad a] \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}$$

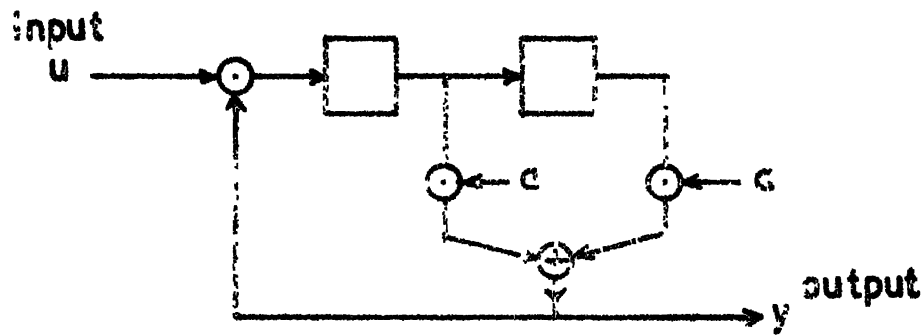


Fig. 3.5.16a $P_2^2 [a^2 + c + 1]$ -LSS of Example 3.5.8

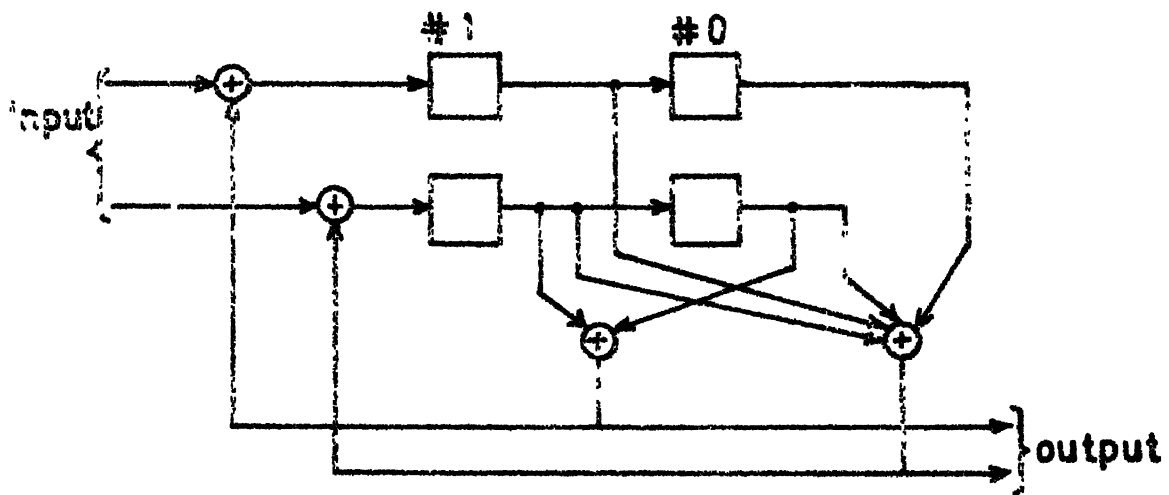


Fig. 3.5.16b $Z_2^2 [W]$ -LSS of Example 3.5.8

where all the entries are from $P_2^2[a^2+a+1]$.

The implementation of $Z_2^2[W]$ -LSS $L' \simeq L$ is given in Figure 3.5.16b.

The corresponding equations of L' are

$$\begin{bmatrix} x'_{00} \\ x'_{01} \\ x'_{10} \\ x'_{11} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{10} \\ x_{11} \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{10} \\ x_{11} \end{bmatrix}$$

This is an example of data scrambler for multilevel pulse sequences proposed in [31] and is not looked from the point of view of $P_p^n[W(a)]$ -LSS.

Example 3.5.9:

Consider the second order $P_2^3[a^3+a+1]$ -LSS, L in Figure 3.5.17a. Since a^3+a+1 is irreducible over $GF(2)$, this is an example of $GF(2^3)$ -LSS.

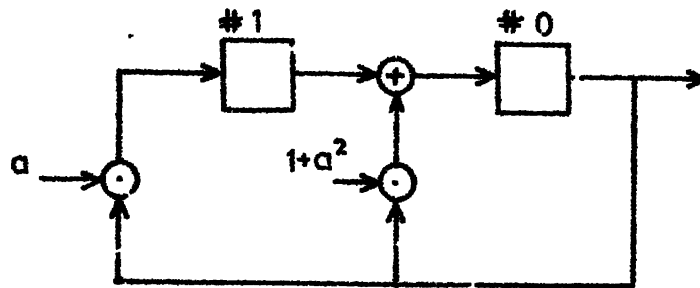


Fig. 3.5.17a $P_2^3[a^3+a+1]$ -LSS of Example 3.5.9

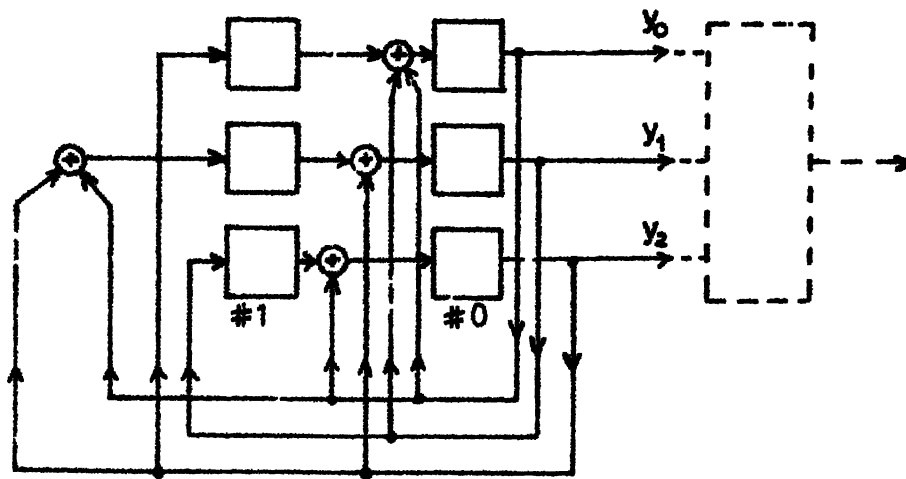


Fig. 3.5.17b $Z_2^3[W]$ -LSS of Example 3.5.9

The state and output equations of this system are,

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1+a^2 & 1 \\ a & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}$$

$$y = [1 \ 0] \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}$$

The $Z_2^3[W]$ -LSS, L' isomorphic to this system can be obtained by writing the state and output equations of L' .

$$\begin{bmatrix} x'_{00} \\ x'_{01} \\ x'_{02} \\ x'_{10} \\ x'_{11} \\ x'_{12} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{02} \\ x_{10} \\ x_{11} \\ x_{12} \end{bmatrix}$$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_{00} \\ x_{01} \\ x_{02} \\ x_{10} \\ x_{11} \\ x_{12} \end{bmatrix}$$

The schematic diagram of L' is given in Figure 3.5.17b.

With additional circuitry shown by dotted lines in Figure 3.5.17b to compute $y^3 + y^6 + y^5$ in $P_2^3[a^3 + a + 1]$, the system is the example of GMW sequence generator proposed by Scholtz and Welch [78] for the generation of binary sequences, with desirable correlation properties. The system then becomes a nonlinear system over residue class polynomial rings, the study of which is not taken up here.

3.6 ISOMORPHISM IN LSS OVER RESIDUE CLASS RING OF POLYNOMIALS OVER $GF(p)$:

In Section 2.4 we have seen that residue class polynomial rings of the same order may be isomorphic to each other. As defined in Section 3.4, if two LSS defined over isomorphic rings are such that there is one-to-one correspondence between their characterising matrices and states, then with isomorphic initial states and isomorphic input sequences, the output sequences of the two LSS will be isomorphic. This leads to the notion of isomorphisms in LSS. In Section 2.6 we have seen that residue class polynomial rings isomorphic to each other constitute an equivalence class. LSS defined over such residue class polynomial rings are said to constitute a distinct class of $P_p^n[W(a)]$ -LSS. $GF(p^n)$ -LSS is one such class. The number of nonisomorphic residue class polynomial rings of a given order then gives the number of distinct classes of LSS over $P_p^n[W(a)]$ of order p^n .

Consider two residue class polynomial rings $P_p^n[W(a)]$ and $P_p^n[W'(a)]$ isomorphic to each other. Then there is one-to-one correspondence between the elements of $P_p^n[W(a)]$ and $P_p^n[W'(a)]$. Let L be a LSS defined over $P_p^n[W(a)]$. Since $P_p^n[W'(a)] \simeq P_p^n[W(a)]$, it is possible to have a LSS L' over $P_p^n[W'(a)]$, such that there is a one-to-one correspondence between the elements of the characterising matrices and hence one-to-one correspondence between the characterising matrices themselves and we say L and L' are isomorphic to each other. That is $A \neq A', B \neq B', C \neq C', D \neq D'$, where A, B, C and D are referred to L and A', B', C' and D' are referred to L' .

It is also possible for L and L' defined over the same structure and be isomorphic, if there is one-to-one correspondence between their characterising matrices.

If L and L' are isomorphic it is always possible to have isomorphic initial states $x(o) \neq \theta(o)$ and isomorphic inputs $u \neq u'$ in which case the outputs are also isomorphic.

The following examples illustrate the notion of isomorphism in $P_p^n[W(a)]$ -LSS.

Example 3.6.1:

Consider two LSS L and L' defined over $P_2^3[a^3+a^2+a]$ and $P_2^3[(b^3+1)]$ respectively. Here $P_2^3[a^3+a^2+a] \simeq P_2^3[(b^3+1)]$. The one-to-one correspondence between the elements of the two rings is given below.

$p_2^3[a^3+a^2+a]$	$p_2^3[b^3+1]$
0	0
1	1
a	b+1
a ²	b ² +1
1+a	b
1+a ²	b ²
a+a ²	b+b ²
1+a+a ²	1+b+b ²

If the state and output equations of L and L' are

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} a & a^2 \\ a^2 & 1+a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a^2 \\ 1+a \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} a^2 & a \\ a & 1+a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 1+a \\ a^2 \end{bmatrix} u$$

and

$$\begin{bmatrix} \theta'_0 \\ \theta'_1 \end{bmatrix} = \begin{bmatrix} 1+b & 1+b^2 \\ 1+b^2 & b \end{bmatrix} \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} + \begin{bmatrix} 1+b^2 \\ b \end{bmatrix} \gamma$$

$$\begin{bmatrix} \delta_0 \\ \delta_1 \end{bmatrix} = \begin{bmatrix} b^2+1 & b+1 \\ 1+b & b \end{bmatrix} \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} + \begin{bmatrix} b \\ 1+b^2 \end{bmatrix} \gamma$$

respectively, then it is seen that the characterising matrices of L are in one-to-one correspondence with the characterising matrices of L' . Hence $L \simeq L'$.

It should be noted that if

$$\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \simeq \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} \quad \text{and} \quad u \simeq \gamma \quad \text{then} \quad \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} \simeq \begin{bmatrix} \delta_0 \\ \delta_1 \end{bmatrix}$$

Example 3.6.2:

Consider two LSS L and L' defined over $P_2^3[a^3+a+1]$ and $P_2^3[b^3+b^2+1]$ respectively. Here $P_2^3[a^3+a+1] \simeq P_2^3[b^3+b^2+1]$. The one-to-one correspondence between their elements is given in Example 2.3.1. If the state and output equations of L and L' are

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ a^2 & 1+a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a \\ 1+a \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} a & a \\ 1 & 1+a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} 1+a \\ a^2 \end{bmatrix} u$$

and

$$\begin{bmatrix} \theta'_0 \\ \theta'_1 \end{bmatrix} = \begin{bmatrix} 1 & 1+b \\ 1+b^2 & b \end{bmatrix} \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} + \begin{bmatrix} 1+b^2 \\ b \end{bmatrix} \gamma$$

$$\begin{bmatrix} \delta_0 \\ \delta_1 \end{bmatrix} = \begin{bmatrix} 1+b & 1+b \\ 1 & b \end{bmatrix} \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} + \begin{bmatrix} b \\ 1+b^2 \end{bmatrix} \gamma$$

respectively, then it is seen that the characterising matrices of L are in one-to-one correspondence with the characterising matrices of L' . Hence $L \simeq L'$.

$$\text{We note that if } \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \neq \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} \text{ and } u \neq \gamma \text{ then } \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} \neq \begin{bmatrix} \delta_0 \\ \delta_1 \end{bmatrix}.$$

The following example illustrates the isomorphisms in $\bigotimes_{\mathbb{I}} \{P_p^{n_i}[W_i(a_i)]\}$ -LSS.

Example 3.6.3:

Consider two LSS L and L' defined over $P_2^2[c^2]$
 $\bigotimes P_2^3[a^3+a^2+a]$ and $P_2^2[(d+1)^2] \bigotimes P_2^3[b^3+1]$
 we have $P_2^2[c^2] \simeq P_2^2[(d+1)^2]$
 and $P_2^3[a^3+a^2+a] \simeq P_2^3[b^3+1]$

The one-to-one correspondence between elements of $P_2^2[c^2]$ and $P_2^2[(d+1)^2]$ are

$P_2^2[c^2]$	0	1	c	1+c
$P_2^2[d^2+1]$	0	1	1+d	d

The one-to-one correspondence between elements of $P_2^3[a^3+a^2+a]$ and $P_2^3[b^3+1]$ is given in Example 3.6.1. Let

a basis of $P_2^2[c^2] \otimes P_2^3[a^3+a^2+a]$ be $\{1, a, a^2, c, ca, ca^2\}$; the corresponding basis of $P_2^2[(d+1)^2] \otimes P_2^3[(b^3+1)]$ is

$$\{1, (b+1), (b^2+1), (d+1), (d+1)(b+1), (d+1)(b^2+1)\}$$

If the state and output equations of L and L' are given by

$$\begin{bmatrix} x'_0 \\ x'_1 \end{bmatrix} = \begin{bmatrix} 1+ca & ca^2 \\ 1+a & c+a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} ca \\ c+a \end{bmatrix} u$$

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1+ca^2 & 1+a \\ 1+ca & c+ca^2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} ca \\ 1+ca^2 \end{bmatrix} u$$

and

$$\begin{bmatrix} \theta'_0 \\ \theta'_1 \end{bmatrix} = \begin{bmatrix} b+d+db & 1+b^2+d+db^2 \\ b & b+d \end{bmatrix} \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} + \begin{bmatrix} 1+b+d+db \\ b+d \end{bmatrix} \gamma$$

$$\begin{bmatrix} \delta_0 \\ \delta_1 \end{bmatrix} = \begin{bmatrix} b^2+d+db^2 & b \\ b+d+db & b^2+db^2 \end{bmatrix} \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} + \begin{bmatrix} 1+b+d+db \\ b^2+d+db^2 \end{bmatrix} \gamma$$

respectively, then it is seen that the characterising matrices of L are in one-to-one correspondence with the characterising matrices of L' . Hence $L \simeq L'$.

If $\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \neq \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix}$ and inputs $u \neq \gamma$ then

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} \neq \begin{bmatrix} \delta_0 \\ \delta_1 \end{bmatrix}$$

Thus if two LSS L and L' are defined over isomorphic rings it is possible for L to be isomorphic to L' .

The following example illustrates the isomorphism between L and L' defined over the same ring.

Example 3.6.4:

Consider the ring $P_2^3[a^3+1]$. Let the characterising matrices of $P_2^3[a^3+1]$ -LSS L be

$$A = \begin{bmatrix} 0 & 1 \\ a^2 & 1+a \end{bmatrix} \quad B = \begin{bmatrix} 1 \\ a \end{bmatrix}; \quad C = \begin{bmatrix} a & 1 \\ a^2 & 1+a \end{bmatrix} \quad D = \begin{bmatrix} 1 \\ a \end{bmatrix}$$

Let $A' = aA$, $B' = aB$, $C' = aC$ and $D' = aD$,

where a is a unit in $P_2^3[a^3+1]$, be characterising matrices of L'

then $A \neq A'$, $B \neq B'$, $C \neq C'$, $D \neq D'$.

and hence $L \cong L'$.

Example 3.6.5:

Let L and L' be defined over the same ring. Suppose Q is an arbitrary $K \times K$ matrix over this ring such that determinant Q is a unit in the ring. Then Q is invertible.

$$\text{Let } A' = QAQ^{-1}$$

$$B' = QB$$

$$C' = CQ^{-1}$$

$$D' = D$$

$$\text{and } \Theta = QX$$

correspond to characterising matrices and state of L' with identical inputs to L and L' ,

we have $X' = AX + Bu$; $y = Cx + Bu$

$$\theta' = A'\theta + B'u = QAQ^{-1}QX + QBu = Q(AX + Bu) = QX'$$

$$y' = C'\theta + D'u = CQ^{-1}QX + Du = CX + Bu = y.$$

Hence the outputs from L and L' are identical for identical inputs.

L and L' are said to be similar LSS. Similar LSS are also isomorphic.

3.6.1 Distinct Classes of $P_p^n[W(a)]$ -LSS:

Residue class polynomial rings which are isomorphic to each other are said to belong to the same class (Section 2.5). Thus in Example 3.6.1, $P_2^3[a^3+a^2+a]$ and $P_2^3[b^3+1]$ are isomorphic and belong to the same class. In Example 3.6.2, $P_2^3[a^3+a+1]$ and $P_2^3[b^3+b^2+1]$ are isomorphic and belong to the same class; indeed they are two isomorphic finite fields of order 2^3 . In Example 3.6.3, $P_2^2[c^2] \otimes P_2^3[(a^3+a^2+a)]$ and $P_2^2[d^2+1] \otimes P_2^3[b^3+1]$ are isomorphic to each other and belong to the same class, and in Example 3.4.2, $P_2^3[a_1^3+1] \otimes P_2^2[a_0^2+1]$ and $P_2^6[a^6+1]$ are isomorphic to each other.

As seen earlier given a LSS over $P_p^n[W(a)]$ it is possible to obtain a LSS L' isomorphic to L over residue

class polynomial ring $P_p^n[W'(b)]$ isomorphic to $P_p^n[W(a)]$. LSS defined over residue class polynomial rings belonging to the same class are said to constitute a class. LSS defined over finite fields of order p^n , constitute one such class. Consider the residue class polynomial rings, $P_2^3[a^3+a^2+a+1]$ and $P_2^3[a^3+1]$. In example 2.5.3 we have seen that these two rings are not isomorphic to each other and therefore belong to different classes. If we have two LSS L and L' of the same order defined over these residue class polynomial rings, as there can not be one-to-one correspondence between their characterising matrices and states, L and L' can not be isomorphic to each other. In this case we say L and L' belong to two different classes of LSS. Thus distinct classes of residue class polynomial rings give rise to distinct classes of LSS. Since finite fields of the same order are all isomorphic to each other the notion of distinct classes does not exist in the case of LSS over finite fields of a given order.

The number of distinct classes of LSS defined over residue class polynomial rings of order p^n is equal to the number of nonisomorphic residue class polynomial rings of order p^n . This number is also equal to the distinct classes of LSS over other commutative rings of order p^n , such as

ring $M_p^n[W]$ of matrices and ring $Z_p^n[W]$ of n -tuples isomorphic to $P_p^n[W(a)]$. Table 2.5.3 in Section 2.5 gives the number of nonisomorphic residue class polynomial rings $P_p^n[W(a)]$ of order p^n for $p = 2, 3, 5$ and $n = 1, 2, 3, 4, 5, 6$ and 7.

If two LSS are defined over residue class polynomial rings belonging to the same class, then the decomposition of the LSS will have same number of subsystems; the corresponding subsystems are over isomorphic orthogonal ideals or primary rings.

CHAPTER 4

AUTONOMOUS RESPONSE OF $P_p^n[W(a)]$ -LSS

It may be recalled that the autonomous response of a $P_p^n[W(a)]$ -LSS is its response when the input is a null sequence. The study of the autonomous response of $P_p^n[W(a)]$ -LSS is important not only because it is a constituent of the total response, but also that it leads to the study of $P_p^n[W(a)]$ -LSS as sequence generators. In this chapter we study the autonomous response of $P_p^n[W(a)]$ -LSS in general and autonomous response of nonsingular single output canonical $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$ in particular; the latter response is shown to satisfy a linear recursion relation over $P_p^n[W(a)]$ and is thus a linear recursion sequence (LRS) over $P_p^n[W(a)]$. The Hamming correlation properties of LRS over $P_p^n[W(a)]$; specially bounds on correlation values of sequences generated by nonsingular $P_p^n[W(a)]$ -LSS are investigated. Sequences over orthogonal ideals, their properties, generation and application of such sequences in modulation and multiplexing of data sequences are studied. The results given here are also valid for LSS over other algebraic structures isomorphic to $P_p^n[W(a)]$. Specifically the results are valid for $Z_p^n[W]$ -LSS and $M_p^n[W]$ -LSS.

Since the autonomous response is a fixed linear transformation of states, we study the state response of $P_p^n[W(a)]$ -LSS in

detail in Section 4.1. The sequence of states which a $P_p^n[W(a)]$ -LSS, passes through, starting from an initial state under zero input condition is usually displayed graphically in the form of a state diagram. In the state diagram, if, starting from any initial state after passing through c other states, $P_p^n[W(a)]$ -LSS reaches the initial state, the sequence of states is said to constitute a cycle of period or length c . Properties of state diagram and state response, module structure of state response, bounds on number of state cycles of a nonsingular system, maximum length state sequences of $P_p^n[W(a)]$ -LSS and state diagrams of isomorphic $P_p^n[W(a)]$ -LSS are discussed.

Cycle length decomposition, Σ , of states of nonsingular $P_p^n[W(a)]$ -LSS is taken up in Section 4.2. Σ depends on the characteristic matrix A and the $P_p^n[W(a)]$ over which the system is defined. Cases where $P_p^n[W(a)]$ is a primary ring and direct sum of primary rings are dealt separately. The period of characteristic matrix A and the number and period of sequences that are available from the system can be obtained from the cycle length decomposition of states.

The autonomous response of $P_p^n[W(a)]$ -LSS is taken up in Section 4.3. It is shown that the autonomous response of a canonical nonsingular K th order $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$ satisfies a linear recursion relation (LRR) of order K over $P_p^n[W(a)]$ and hence is a linear recursion sequence (LRS) over

$P_p^n[W(a)]$. The autonomous response can be obtained in terms of the initial state and powers of matrix A or in terms of initial state and generating function. It is shown that the set of solutions of LRR over $P_p^n[W(a)]$ constitutes a free module of rank K .

One of the important properties of sequences in applications such as modulation, and multiplexing of data sequences, is their correlation property. The concept of Hamming metric, Hamming distance, Hamming cross-correlation (HCCR) function between sequences and Hamming autocorrelation (HACR) function of sequences are discussed in Section 4.4. The bounds on values of HCCR and HACR functions of sequences, generated by autonomous single output LSS are obtained, utilising structure of state cycles or from the state diagram. Expressions for the actual values and the number of levels of HACR and HCCR functions for specific cases are given. Examples of weight enumeration of the sequences of length T , which are solutions of a specific class of second order LRR are also given. HCCR property of sequences over $P_p^n[W(a)]$ is used in decoding cyclic codes in Chapter 5.

The orthogonal idempotents in semisimple or semilocal $P_p^n[W(a)]$ generate proper ideals in $P_p^n[W(a)]$. For convenience we have called these ideals as orthogonal ideals. Elements from different orthogonal ideals annihilate each other. Thus sequences over orthogonal ideals have pointwise orthogonal

property. Such sequences can be applied in modulation and multiplexing of data sequences. In Section 4.5, generation of orthogonal sequences in appropriate $P_p^n[W(a)]$ -LSS, and using the notion of decomposition of $P_p^n[W(a)]$, decomposition of arbitrary sequences over semisimple or semilocal ring into orthogonal sequences over orthogonal ideals, transformation of sequence over semisimple or semilocal ring into a set of orthogonal sequences over orthogonal ideals in an appropriate semisimple or semilocal ring by ring embedding are presented.

Application of orthogonal sequences in modulation and multiplexing of data sequences with elements from finite fields are given in Section 4.6.

To begin with, we recall some of the definitions introduced earlier in Section 3.2. Unless otherwise specified, by LSS we mean $P_p^n[W(a)]$ -LSS.

4.1 AUTONOMOUS STATE RESPONSE OF $P_p^n[W(a)]$ -LSS

Consider an m -input and j -output $P_p^n[W(a)]$ -LSS of order K , with characteristic matrix A . The sequence of output j -tuples of the LSS, when the sequence of input m -tuple is a null sequence, is called its autonomous response and a LSS with null sequence as input is called an autonomous LSS. Sequence of states through which the LSS passes through with null sequence as input is called autonomous state response.

As seen in Chapter 3, expressions for Nth element of autonomous state response and autonomous response are

$$x_{ZIR}(N) = A^N x(o) \quad (4.1.1)$$

$$y_{ZIR}(N) = CA^N x(o) \quad (4.1.2)$$

If $x(o) = 0$, i.e., a K-tuple of all zeros in $P_p^n[W(a)]$, the autonomous state response $\{x_{ZIR}(N)\}$ is a sequence of 0's and the autonomous response $\{y_{ZIR}\}$ is a sequence of j-tuples which are all zeros in $P_p^n[W(a)]$.

For the sake of convenience, in this chapter we make use of the following conventions:

- (i) $x_{ZIR}(N), y_{ZIR}(N)$ are denoted simply as x_N and y_N
- (ii) A $P_p^n[W(a)]$ -LSS is denoted by L , and
- (iii) Autonomous state response is simply called state response.

4.1.1 State Diagram of Autonomous LSS

The relevant information regarding the state response of a given L for all possible values of x_o is conveniently displayed in the form of state diagram which is an oriented (or directed) graph with p^{nK} vertices, one for each state of L , an arrow points from state x_1 to x_2 iff $x_2 = Ax_1$ and we say that x_1 is a predecessor of x_2 or x_2 is a successor of x_1 . Thus, given any specified initial state, the state diagram displays the sequence

of states through which L goes for the zero input.

A state x_a is called a cyclic state, if there exists an integer c_a , such that $x_a = A^{c_a} x_a$. If c_a is the least integer that satisfies this condition, then the sequence $x_1 = A x_a$; $x_2 = A^2 x_a$; ..., $x_{(c_a-1)} = A^{(c_a-1)} x_a$; $x_{c_a} = A^{c_a} x_a = x_a$ of distinct states is called a state cycle (or simply a cycle), of length or period c_a . Such a state cycle will be denoted by

$$(x_1, x_2, \dots, x_{c_a-1}, x_{c_a})$$

or any of its cyclically shifted version such as

$$(x_2, x_3, \dots, x_{c_a-1}, x_{c_a}, x_1)$$

$$(x_4, x_5, \dots, x_{c_a-1}, x_{c_a}, x_1, x_2, x_3)$$

$$(x_{c_a} = x_a, x_1, x_2, \dots, x_{c_a-1}) .$$

c_a is also called the period of state sequence. Zero state is always a cyclic state of length 1.

A state x_b is called a noncyclic or transient state if x_b is not equal to $A^j x_b$ for any $j = 1, 2, \dots$

A state diagram or a portion of it consisting of set of states terminating in a single cyclic state of length one, (other states being noncyclic) is called a tree. The terminating cyclic state is called the root of the tree.

Before taking up the properties of state diagram and hence the state response, we give some terminology and illustrative examples.

A sequence of the form

$$\{x\} = (x_0, x_1, x_2, 0, 0, \dots, 0) \quad (4.1.3)$$

is called an ultimately zero sequence.

A sequence of the form

$$\{x\} = (x_0, x_1, \dots, x_{\tau-1}, x_{\tau}, x_{\tau+1}, \dots, x_{\tau+T-1}, x_{\tau}, x_{\tau+1}, \dots) \quad (4.1.4)$$

is said to be an ultimately periodic sequence. The part of the sequence $(x_0, x_1, \dots, x_{\tau-1})$ is the transient part; τ is called the length of transient. T is called the period of the periodic portion of the sequence. If $\tau = 0$, the sequence $\{x\}$ given by (4.1.4) is said to be periodic with period T .

Example 4.1.1

Consider a 2nd order $P_2^2[a^2+a]$ -LSS with $A = \begin{bmatrix} a & a \\ 1 & a \end{bmatrix}$ over semisimple $P_2^2[a^2+a]$, $|A| = 0$. Further $A^2 = \underline{0}$. Hence A is singular and nilpotent. The index of nilpotence is 2. The state diagram is a tree with root $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$, as given in Figure 4.1.1. With any initial state, the state response ultimately becomes a sequence of zeros. The state response is then called an ultimately zero sequence.

For example, with $\begin{bmatrix} a \\ 0 \end{bmatrix}$ as initial state, the state response is $\left(\begin{matrix} a & a & 0 & 0 \\ 0 & 0 & 0 & 0 \end{matrix} , \dots \right)$ which is an ultimately zero sequence.

Example 4.1.2

Consider a 2nd order $P_2^2[a^2+a]$ -LSS with $A = \begin{bmatrix} 1 & 1+a \\ a & 1+a \end{bmatrix}$;

$|A| = (1+a)$ is a zero divisor in semisimple $P_2^2[a^2+a]$. Hence A is singular. The state diagram of this LSS is given in Fig. 4.1.2. It has $(2^2)^2 = 16$ states. Since A is singular all the states are not cyclic. The noncyclic states are

$$\left(\begin{matrix} 1 & a & 0 & 1+a & 1+a & 0 & a & 1 \\ , & , & , & , & , & , & , & , \\ 0 & 0 & a & a & 1 & 1 & 1+a & 1+a \end{matrix} \right) . *$$

If the initial state is a noncyclic state which terminates in a state cycle of length c , the state response becomes ultimately periodic with period equal to the period c of the state cycle. The number of noncyclic states in the initial portion of state response is the length of transient.

For instance, in LSS of Example 4.1.2 with initial state

$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, which is noncyclic, the state response is

$$\left(\begin{matrix} 1 & 1 & 1 \\ , & , & , \\ 0 & a & a \end{matrix} , \dots \right)$$

which is ultimately periodic with period 1 and length of transient 1. With initial state $\begin{bmatrix} 0 \\ a \end{bmatrix}$ the state response is

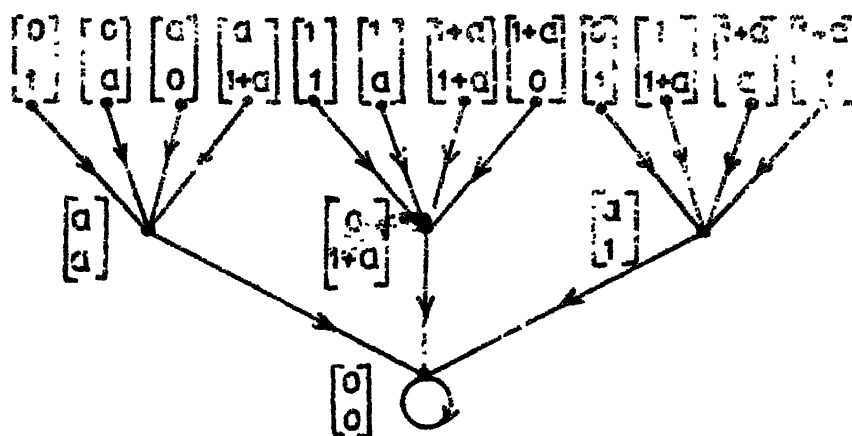


Fig.4.1.1 State diagram of LSS of Example 4.1.1

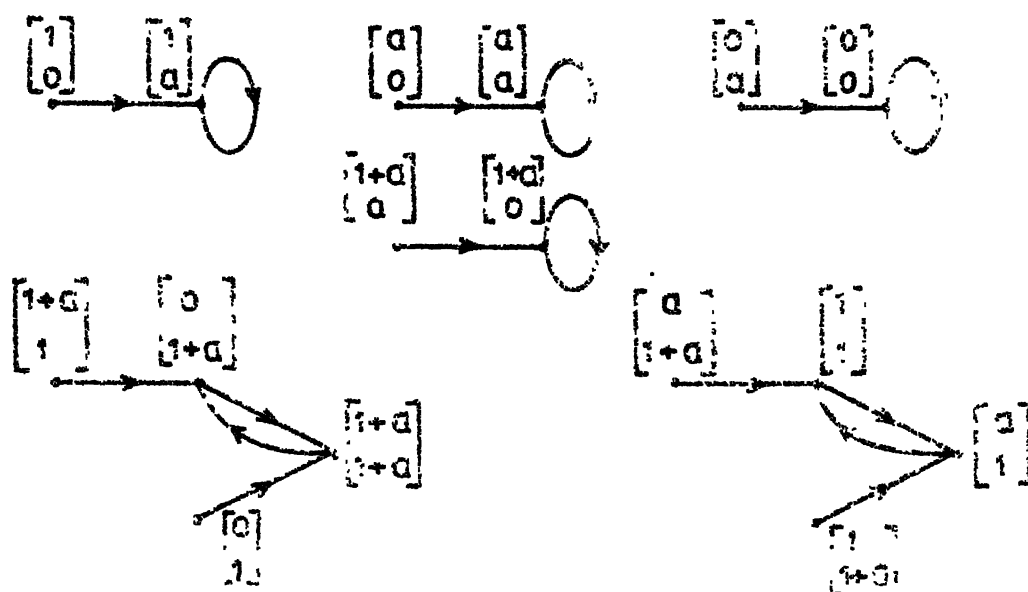


Fig.4.1.2 State diagram of LSS of Example 4.1.2

$$\begin{pmatrix} 0 & & 0 & & 0 & & \dots \\ a & & 0 & & 0 & & \dots \end{pmatrix}$$

which is ultimately periodic with period 1 and length of transient 1. Further the state response is ultimately a zero sequence.

If the initial state is a cyclic state, which is in a state cycle of period c , then the state response is periodic with period c . With initial state $\begin{bmatrix} a \\ 1 \end{bmatrix}$, which is cyclic, the state response of LSS of Example 4.1.2 is

$$\begin{pmatrix} a & 1 & a & \dots \\ 1 & 1 & 1 & \dots \end{pmatrix},$$

which is periodic with period 2.

*

Example 4.1.3

Consider a 2nd order $P_2^2[a^2+a]$ -LSS with $A = \begin{bmatrix} 1 & 1+a \\ a & 1 \end{bmatrix}$;

$|A| = 1$ which is a unit in the semisimple $P_2^2[a^2+a]$. A is nonsingular. The state diagram of this LSS is given in Figure 4.1.3. It has $(2^2)^2 = 16$ states and all states are cyclic states. Period T of matrix $A = \text{lcm}(2,1) = 2$.

The state diagram consists of 10 cycles. They are

$$\begin{pmatrix} 1 & 1 \\ 0 & a \end{pmatrix}; \begin{pmatrix} 0 & 1+a \\ 1 & 1 \end{pmatrix}; \begin{pmatrix} 1 & a \\ 1+a & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1+a \\ 1+a & 1+a \end{pmatrix};$$

$$\begin{pmatrix} a & a \\ 0 & a \end{pmatrix}; \begin{pmatrix} 1 & a \\ 1 & 1+a \end{pmatrix}; \begin{pmatrix} 0 \\ a \end{pmatrix}; \begin{pmatrix} 0 \\ 0 \end{pmatrix}; \begin{pmatrix} 1+a \\ 0 \end{pmatrix}; \begin{pmatrix} 1+a \\ 0 \end{pmatrix}$$

In this case, since all the states are cyclic the state response is periodic irrespective of initial state. For example with initial state $\begin{bmatrix} a \\ 1 \end{bmatrix}$, the state response is

$$\begin{pmatrix} a & 1 & a & \dots \\ 1 & 1+a & 1 & \dots \end{pmatrix}$$

with period 2.

Example 4.1.4

Consider a 2nd order $P_2^2[a^2+1]$ - LSS with $A = \begin{bmatrix} 1 & 1 \\ a & 1+a \end{bmatrix}$ over local $P_2^2[a^2+1]$ we have $|A| = 1$. Hence A is nonsingular. The state diagram of this LSS is given in Figure 4.1.4. It has $(2^2)^2 = 16$ states which are cyclic. Period T of matrix $A = \text{lcm}(6, 3, 1) = 6$.

The state diagram consists of 4 cycles. The cycles are

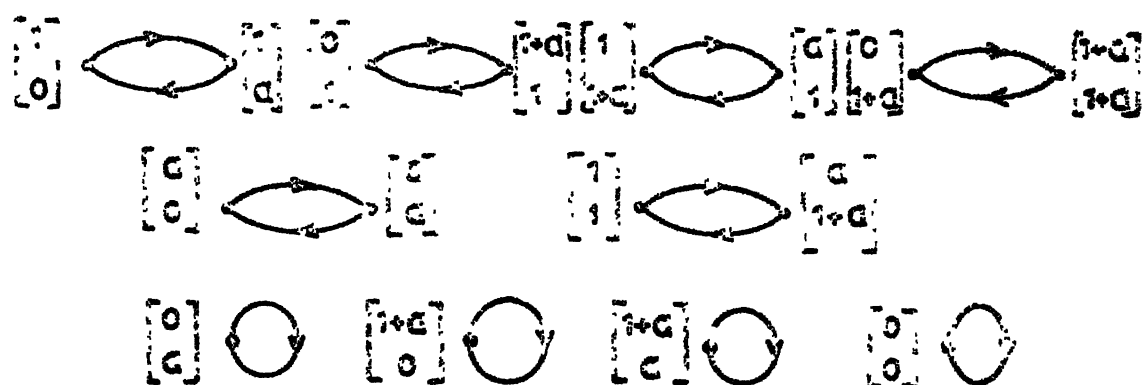


Fig.4.1.3 State diagram of LSS of Example 4.1.3

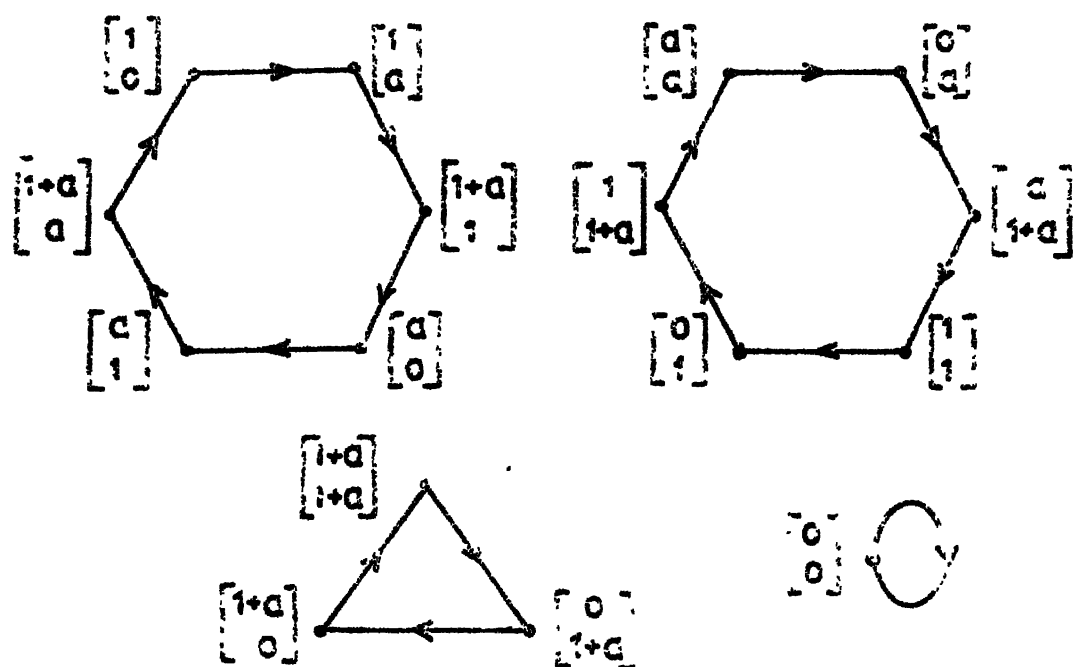


Fig.4.1.4 State diagram of LSS of Example 4.1.4

$$\begin{pmatrix} 1 & 1 & 1+a & a & a & 1+a \\ 0 & a & 1 & 0 & 1 & a \end{pmatrix} ; \\
 \begin{pmatrix} a & 0 & a & 1 & 0 & 1 \\ a & a & 1+a & 1 & 1 & 1+a \end{pmatrix} ; \\
 \begin{pmatrix} 1+a & 0 & 1+a \\ 1+a & 1+a & 0 \end{pmatrix} ; \quad \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

With any initial state the state response is periodic. *

4.1.2 General Properties of State Diagram and State Response

It is seen from the examples that the nature of the state diagram depends on the matrix A . Depending upon the nature of A , the states are either cyclic or noncyclic and the state diagram is cyclic or an appropriate combination of cyclic and noncyclic states. Since the state response $\{x\}$ is the sequence of states through which the system goes in response to a specified initial state x_0 , it depends on both the characteristic matrix A and the initial state x_0 . If A is nilpotent, then with any initial state the state diagram is a tree, and the state sequence x_0, Ax_0, A^2x_0, \dots , ultimately becomes a zero sequence. If A is singular, then depending on the initial state (i) the state diagram is cyclic in which case the state sequence is periodic, or (ii) the state diagram consists of noncyclic states terminating in a cycle in which case the state

sequence is ultimately periodic. If A is nonsingular all the states are cyclic. Hence, irrespective of initial state the state sequence is periodic. Nature of state response is summarised in Table 4.1.1. In what follows, we prove the statements given in Table 4.1.1 and give other general results on the structure of state diagram and state response of a K th order autonomous $P_p^n[W(a)]$ -LSS.

Lemma 4.1.1

- (a) The nonzero states of a nilpotent LSS are noncyclic and the state diagram of such a system is accordingly a tree.
- (b) The state response of a nilpotent system is ultimately a zero sequence.

Proof

We prove the Lemma by contradiction. Let A be nilpotent of order v i.e., v is the least integer such that $A^v = 0$. If a nonzero state x is cyclic with cycle length c , then we should have

$$x, Ax, A^2x, \dots, A^c x = x$$

Three cases may arise

$$c = v; \quad c > v; \quad c < v$$

i) $c = v$:

$$\text{then } A^c x = A^v x = 0 \neq x$$

Table 4.1.1 Nature of State Cycles and State Response

Nature of A	Nature of State cycles	Nature of State response	Remarks
Singular and nilpotent	All the states except 0 are noncyclic	Ultimately zero sequence	Irrespective of initial state
Singular but not nilpotent	Mixture of cyclic and noncyclic states	Ultimately zero or ultimately periodic or periodic	Depends on initial state
Nonsingular	All the states are cyclic	Periodic	Irrespective of initial state

ii) $c > v : A^j = \underline{0}$ for all $j > v$

therefore, $A^c x = 0 \neq x$

iii) $c < v$

$$A^c x = x$$

Hence $A^{jc} x = x$, j any integer.

Let j be such that $jc > v$, then

$$A^{jc} x = \underline{0} \neq x$$

Thus in all the three cases, the hypothesis that the nonzero state x is a cyclic state with period c is contradicted.

Since x has been taken as an arbitrary nonzero state, it is proved that all the nonzero states are noncyclic. Further it is seen that all the nonzero states terminate in the zero state. Therefore, the sequence of states,

x, Ax, A^2x, \dots ultimately reaches zero state for any starting nonzero state x . Hence the state diagram is a tree with the zero state as its root.

*

Lemma 4.1.2

(a) The states of a singular LSS are both cyclic and noncyclic and the state diagram consists of appropriate combination of cycles, trees, and noncyclic states terminating on cycles. If A is idempotent all noncyclic states terminate on a cyclic state of length 1.

(b) The state response of a singular system is an ultimately periodic sequence.

Proof :

Since A is singular A^{-1} is not defined. Hence the predecessor of a state is not unique. A state may have no predecessor, one predecessor or more than one predecessor.

As seen in Section 3.3,1 since A is over a ring $P_p^n[W(a)]$ of finite order, for some least integers i and j and for some initial state x

$$A^i x = A^j x$$

and hence the states $A^i x, A^{i+1} x, \dots, A^j x = A^i x$ constitute a cycle. Hence a state must eventually reach a cycle of states regardless of the initial state; and the state response is ultimately a periodic sequence.

When A is idempotent, $A^2 = A$. This implies that if x is a noncyclic state, its next state is Ax and $A^2 x = Ax$. Hence noncyclic state terminates on a cyclic state of length 1.

Lemma 4.1.3

*

- a) All the states of a nonsingular LSS are cyclic and the state diagram consists of disjoint cycles.
- b) The state response of nonsingular LSS is periodic. The period of the state response is equal to the cycle length of the state cycle containing the initial state x_0 .

Proof

The characteristic matrix A is nonsingular. Hence for an initial state say x_1 , if $x_2 = Ax_1$ then $x_1 = A^{-1} x_2$. This implies each state has a unique predecessor. Since A is deterministic each state has a unique successor. In the state diagram only one arrow points from each state and one arrow points towards each state. Thus all the states are cyclic. No state is common for two state cycles. Hence the state cycles are disjoint.

b) Since all the states are cyclic, the state sequence is periodic irrespective of the initial state. The period of state response with initial state x is the least integer c such that $A^c x = x$, which is also equal to the cycle length of state cycle.

Additional properties of nonsingular LSS are given in the following theorems.

•*

Theorem 4.1.1

In a nonsingular LSS, the cycle length and hence, the period of state sequence divide the period T of characteristic matrix.

Proof : Let x_1 be a state in the state cycle of length c_1 or state sequence of period c_1 . Then c_1 is the least integer such that

$$A^{c_1} x_1 = x_1$$

$$A^T = I$$

Therefore, $A^T x_1 = x_1$

Suppose c_1 does not divide T .

Then let $T = c_1 q + r \quad r < c_1$

$$x_1 = A^T x_1 = A^{c_1 q + r} x_1 = A^r A^{c_1 q} x_1 = A^r x_1$$

This implies that, period of x_1 is $r < c_1$. Since period of x_1 is assumed to be c_1 this is a contradiction. Therefore, r has to be zero and $T = c_1 q$ and $c_1 | T$. *

We have obtained expressions in Section 3.3, for the period T of the matrix A , depending on the ring over which A is defined. The period T can also be obtained from the length of state cycles as proved in the following theorem.

Theorem 4.1.2

If the state diagram of nonsingular LSS has cycles of period c_1, c_2, \dots, c_r , then the period T of A is given by $T = \text{lcm}(c_1, c_2, \dots, c_r)$.

Proof : T is the period of A . Hence, $A^T x = x$ for all x .

T is a multiple of $\text{lcm}(c_1, c_2, \dots, c_r)$.

By definition T is the least integer such that

$$A^T = I$$

Hence, $T = \text{lcm}(c_1, c_2, \dots, c_r)$. *

Example 4.1.5

Referring to the LSS of Example 4.1.3, the lcm of state periods is 2 and the period of characteristic matrix

$$A = \begin{bmatrix} 1 & 1+a \\ a & 1 \end{bmatrix} \text{ over semisimple } P_2^2[a^2+a] \text{ is 2.}$$

*

Example 4.1.6

Referring to the LSS of Example 4.1.4 the lcm of state periods is 6, and the period of characteristic matrix

$$A = \begin{bmatrix} 1 & 1 \\ a & 1+a \end{bmatrix}, \text{ over local } P_2^2 = [a^2+1], \text{ is 6.}$$

*

Theorem 4.1.3

If the initial state x_0 has components from a single ideal J in $P_p^n[W(a)]$, then the states in the sequence, Ax_0 , A^2x_0 , ..., have components from J .

Proof : The components of the successive states are the linear combination over $P_p^n[W(a)]$ of the components of the initial state, which are from an ideal. Since the multiplication of any element in J with any element in $P_p^n[W(a)]$ gives an element in J and J is closed under addition the states in the sequence,

$$Ax_0, A^2x_0, \dots$$

will have components from J .

*

Referring to Example 4.1.3, $J = \{0, 1+a\}$ is an ideal in $P_2^2[a^2+1]$. Initial state with elements from J will have successive states with elements from the same ideal. For example with the initial state $\begin{bmatrix} 1+a \\ 1+a \end{bmatrix}$ the state sequence is

$$\begin{pmatrix} 1+a & 0 & 1+a & \dots \\ 1+a & 1+a & 0 & \dots \end{pmatrix}$$

Having discussed the nature of state sequence and other properties of nilpotent, singular and nonsingular $P_p^n[W(a)]$ -LSS, we now take up some additional properties of state sequences of $P_p^n[W(a)]$ -LSS, which depend on the specific structure of $P_p^n[W(a)]$. When $P_p^n[W(a)]$ is a semisimple ring that is, $W(a)$ is a product of ν irreducible polynomials, we have seen in Section 2.4 that $P_p^n[W(a)]$ has ideals J_1, J_2, \dots, J_ν generated by orthogonal idempotents $e_i(a)$; $i = 1, 2, \dots, \nu$. The state cycles then have additional structure given by

Theorem 4.1.4.

If $P_p^n[W(a)]$ is semisimple and the elements of A are from an ideal J_i generated by one of the orthogonal idempotents $e_i(a)$ in $P_p^n[W(a)]$ and $|A| \neq 0$, then

- i) if the initial state x_0 has components from J_i , the state cycle containing x_0 and hence the state sequence x_0, Ax_0, A^2x_0, \dots is periodic, ii) if the initial state x_0 has

components from J_j ; $j \neq i$, the next state is a zero state and the state sequence is ultimately zero, iii) for arbitrary initial state x_0 with at least one component a unit in $P_p^n[W(a)]$ the state cycle will have one noncyclic state x_0 and the state sequence is ultimately periodic.

Proof : i) We have seen in Section 2.4 that

$$J_i \simeq P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$$

$|A| \neq 0$ and A is over J_i whose order is finite.

Hence there exists an integer T_i such that

$$A^{T_i} = \begin{bmatrix} e_i(a) & & \\ & \ddots & \\ & & e_i(a) \end{bmatrix}$$

and A is not a nilpotent matrix.

If x_0 has components from J_i then

$$A^{T_i} x_0 = \begin{bmatrix} e_i(a) & & \\ & \ddots & \\ & & e_i(a) \end{bmatrix} x_0 = x_0$$

Hence the state sequence x_0, Ax_0, A^2x_0, \dots , is periodic.

ii) Elements of A are multiple of $e_i(a)$. Elements of x_0 are multiple of any $e_j(a)$; $j \neq i$. As seen in Section 2.4

$e_j(a) \cdot e_i(a) = 0$; $j \neq i$, Hence $Ax_0 = 0$ and the state sequence is ultimately zero sequence.

iii) x_0 has at least one component which is a unit in $P^n_P[W(a)]$. But Ax_0 has all the components from J_1 . From (i) the sequence Ax_0, A^2x_0, \dots is periodic. Hence only x_0 is a noncyclic state leading to the cyclic states

$$Ax_0, A^2x_0, \dots$$

and the state sequence is ultimately periodic. *

The application of theorem 4.1.4 is illustrated in the following example.

Example 4.1.7

Consider $A = \begin{bmatrix} 0 & 1+a \\ 1+a & 1+a \end{bmatrix}$ over the semisimple ring

$P_2^2[a^2+a]$. $|A| = 1+a$ is a zero divisor in $P_2^2[a^2+a]$, but is an element in the ideal $J_1 = \{0, (1+a)\}$ generated by the orthogonal idempotent $(a+1)$.

Suppose the initial state is $x_0 = \begin{bmatrix} 1+a \\ 0 \end{bmatrix}$, then the state cycle containing x_0 has states Ax_0, A^2x_0 with elements from J_1 as shown in Figure 4.1.5a. If the initial state x_0 has elements from $J_1 = \{0, a\}$ generated by orthogonal idempotent a in $P_2^2[a^2+a]$, then the next state is zero as shown in Figure 4.1.5b.

For any other arbitrary initial state say $x_0 = \begin{bmatrix} 1 \\ a \end{bmatrix}$, we have the sequence of states which has only one noncyclic state $x_0 = \begin{bmatrix} 1 \\ a \end{bmatrix}$, as shown in Figure 4.1.5c.

*

Additional properties of state cycles when $P_p^n[W(a)]$ is a semilocal ring, that is, $W(a)$ is a product of powers of irreducible polynomials, are proved in the following theorem.

Theorem 4.1.5

If $P_p^n[W(a)]$ is semilocal and the elements of A are from an ideal J_i generated by one of the orthogonal idempotents $e_i(a)$ in $P_p^n[W(a)]$ then, (i) if $|A|$ is a nilpotent in J_i the sequences are ultimately periodic or ultimately zero, (ii) if $|A|$ is not a nilpotent in J_i , if the initial state has components from J_i the sequence is periodic; if the initial state has components with atleast one unit from $P_p^n[W(a)]$, then the sequence is ultimately periodic with transient of length atmost one.

Proof :

We make use of the isomorphism between J_i and local ring $P_p^{h_i n_i i}[W_i^{h_i i}(a)]$ to prove the theorem.

Let $K \times K$ matrix A be over J_i . Let $\phi: J_i \rightarrow P_p^{h_i n_i i}[W_i^{h_i i}(a)]$. Then $\phi(A)$ has elements from $P_p^{h_i n_i i}[W_i^{h_i i}(a)]$. Since $P_p^{h_i n_i i}[W_i^{h_i i}(a)]$ is a local ring, the zero divisors in this ring are also nilpotent

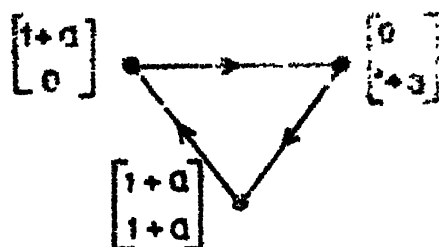


Fig.4.1.5 a State diagram with initial state $\begin{bmatrix} 1+a \\ 0 \end{bmatrix}$

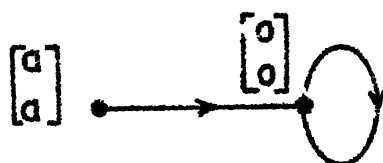


Fig.4.1.5b State diagram with initial state $\begin{bmatrix} a \\ a \end{bmatrix}$

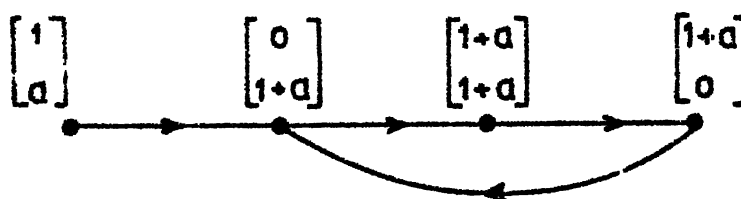


Fig.4.1.5c State diagram with initial state $\begin{bmatrix} 1 \\ a \end{bmatrix}$

elements. Thus nilpotent elements in J_i have one-to-one correspondence with zero divisors in $P_p^{h_i n_i}[W_i(a)]$. If $|A|$ is a nilpotent in J_i then $|\phi(A)|$ is a zero divisor in $P_p^{h_i n_i}[W_i(a)]$ and state sequences are ultimately periodic or ultimately zero. Thus the sequences over J_i are also ultimately periodic or ultimately zero.

ii) If $|A|$ is not a nilpotent in J_i then $|\phi(A)|$ is a unit in $P_p^{h_i n_i}[W_i(a)]$ and thus the sequences are periodic for all initial values from $P_p^{h_i n_i}[W_i(a)]$. Thus for this case if the initial values are from J_i the state sequences are periodic. If the initial state is from $P_p^n[W(a)]$ with at least one unit from $P_p^n[W(a)]$, then the next state has elements from J_i . Hence state sequence is periodic with transient at most one.

*

4.1.3 Module Structure of State Response

Now we show that the set of all state sequences corresponding to an autonomous $P_p^n[W(a)]$ -LSS constitutes a free $P_p^n[W(a)]$ -module of rank K . Towards this end we first prove the following Lemma.

Lemma 4.1.4

Each initial state of a K th order $P_p^n[W(a)]$ -LSS gives rise to a unique state sequence.

Proof :

A K th order $P_p^n[W(a)]$ -LSS has p^{nK} distinct states. There

are thus p^{nK} distinct initial states. In the state sequence with initial state x , the first state is the state x itself. Thus each distinct initial state gives rise to a state sequence, with distinct first component, and hence a unique state sequence. *

Theorem 4.1.6

Set S_s of all state sequences constitute a free $P_p^n[W(a)]$ module of rank K .

Proof :

We first prove that the set S_s of all state sequences constitutes a $P_p^n[W(a)]$ -module.

S_s is an additive abelian group under pointwise addition modulo $[p; W(a)]$ of components of states. The zero state is the additive identity.

Let $x = (x_0, x_1, x_2, x_3, \dots)$

and $z = (z_0, z_1, z_2, z_3, \dots)$

be state sequences with initial state x_0 and z_0 respectively in S_s . Let $l, b_1, b_2, b \in P_p^n[W(a)]$.

S_s satisfies the following module axioms.

$$\begin{aligned}
 \text{i) } b(\{x\} + \{z\}) &= b(x_1+z_1, x_2+z_2, \dots) \\
 &= (bx_1+bz_1, \quad bx_2+bz_2, \dots) \\
 &= b \{x\} + b \{z\} .
 \end{aligned}$$

$$\begin{aligned}
 \text{ii)} \quad (b_1+b_2) \{x\} &= ((b_1+b_2)x_1, (b_1+b_2)x_2, (b_1+b_2)x_3, \dots) \\
 &= (b_1x_1+b_2x_1, b_1x_2+b_2x_2, b_1x_3+b_2x_3, \dots) \\
 &= b_1\{x\} + b_2\{x\}
 \end{aligned}$$

$$\begin{aligned}
 \text{iii)} \quad b_1b_2 \{x\} &= (b_1b_2x_1, b_1b_2x_2, b_1b_2x_3, \dots) \\
 &= (b_1(b_2x_1), b_1(b_2x_2), \dots) \\
 &= b_1(b_2\{x\})
 \end{aligned}$$

$$\begin{aligned}
 \text{iv)} \quad 1 \{x\} &= (1x_1, 1x_2, 1x_3, \dots) \\
 &= (x_1, x_2, x_3, \dots) \\
 &= \{x\}
 \end{aligned}$$

Thus S_s is a $P_p^n[W(a)]$ -module.

We now prove that S_s is a free module of rank K .

Consider the set of K states

$$\begin{pmatrix} 1 & 0 & 0 & & 0 \\ 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \quad (4.1.5)$$

Each state gives rise to a unique state sequence in S_s .

Any initial state can be expressed as a linear combination over $P_p^n[W(a)]$ of these K states uniquely. Hence any state sequence in S_s can be expressed as the linear combination over $P_p^n[W(a)]$ of the K sequences with initial states given in set (4.1.5), uniquely. This implies S_s is free and is of rank K .

Lemma 4.1.5

*

The module of states S_x is isomorphic to module of state sequences S_s .

Proof :

The set S_x of p^{nK} states is a free module of rank K . The set S_s of p^{nK} sequences is also a free module of rank K . There is a one-to-one correspondence between states in S_x and sequences in S_s . Hence $P_p^n[W(a)]$ -module S_x is isomorphic to $P_p^n[W(a)]$ -module S_s .

*

4.1.4 Bounds on the Number of State Cycles and Maximal Length
State Sequences of Nonsingular $P_p^n[W(a)]$ -LSS

We show that the number of nontrivial cycles in the state diagram of a $P_p^n[W(a)]$ -LSS which is not isomorphic to a $GF(p^n)$ -LSS, is always greater than one. Bounds on the minimum number of state cycles in the state diagram of a nonsingular $P_p^n[W(a)]$ -LSS are obtained. Actual structure of state cycles has been taken up separately in Section 4.2.

Since the number of nonzero states in a K th order $P_p^n[W(a)]$ -LSS is $(p^{nK}-1)$ and the number of nontrivial cycles is greater than one, the length of state cycles and hence period of state sequence of $P_p^n[W(a)]$ -LSS is always less than $(p^{nK}-1)$. If T is the period of the characteristic matrix A of the $P_p^n[W(a)]$ -LSS, there exists at least one initial state such that the period of state sequence is T . This result is then used to obtain results concerning the maximal possible period of states of $P_p^n[W(a)]$ -LSS which gives rise to the notion of maximum length state sequences. For the sake of comparison of different $P_p^n[W(a)]$ -LSS of the same order, from the consideration of maximum possible period of state sequence, a figure of merit F for the $P_p^n[W(a)]$ -LSS is defined.

To obtain the bound on the minimum number of state cycles, we first prove the following lemma.

Lemma 4.1.6

Consider a nonsingular $P_p^n[W(a)]$ -LSS where $W(a) = \prod_{i=1}^v w_i^{h_i}(a)$. The number of nontrivial state cycles with components of states from ideals in $P_p^n[W(a)]$ only is

$$\geq h = \left[\prod_{i=1}^v (h_i + 1) \right] - 2.$$

Proof :

From Theorem 4.1.3 if a state cycle has an initial state with components from an ideal J , then all the states in the

cycle have elements from the same ideal. From Theorem 2.2.1, the number of proper ideals in $P_p^n[W(a)]$ is $h = \left[\sum_{i=1}^v \pi (h_i+1) \right] - 2$.

Thus there are at least h initial states each with components from one of these h ideals. The h initial states will be in h different state cycles. Thus the number of nontrivial state cycles with elements from ideals only is

$$\geq h = \left[\sum_{i=1}^v \pi (h_i+1) \right] - 2$$

*

The following corollaries directly follow from Lemma 4.1.6.

Corollary 4.1.1

When $W(a) = W_1^{h_1}(a)$, where $W_1(a)$ is irreducible polynomial over $GF(p)$ the number of nontrivial state cycles with elements from ideals only is

$$\geq (h_1 - 1)$$

*

Corollary 4.1.2

When $W(a) = \sum_{i=1}^v W_i(a)$ where $W_i(a)$ is irreducible polynomial over $GF(p)$, the number of nontrivial state cycles with elements from ideals only is $\geq (2^v - 2)$. The Lemma 4.1.6 is now used to establish the following Theorem.

*

Theorem 4.1.7

Consider a nonsingular $P_p^n[W(a)]$ -LSS. If the number of ideals in $P_p^n[W(a)]$ is h , then the number of state cycles is $> h$.

Proof :

From the result of Lemma 4.1.6 there are at least h state cycles with components of states from ideals only. The elements of ideals are zero divisors. Consider a state x with at least one component a unit. This state will not lie in any of the h state cycles. Further since the system is nonsingular x lies in a state cycle. Therefore, the number of state cycles in a nonsingular LSS is $> h$.

*

If $W(a)$ is irreducible, $P_p^n[W(a)]$ is a field and the maximum possible period of $K \times K$ characteristic matrix A , over $P_p^n[W(a)]$ is $(p^{nK}-1)$, (it is the period of minimal polynomial of A); thus the maximum possible period of state cycle is $(p^{nK}-1)$. However, if $W(a)$ is reducible, then the number of nontrivial cycle is $> h$ and since the total number of states is p^{nK} , no state cycle of a $P_p^n[W(a)]$ -LSS will have a period equal to $(p^{nK}-1)$.

From Theorem 4.1.1, it is seen that the period of state cycle and hence state sequence, divide the period T of characteristic matrix A . Thus the period of state sequence can be at most T .

As we shall see, for a canonical nonsingular $P_p^n[W(a)]$ -LSS, there is at least one state cycle with period equal to T .

In what follows we consider canonical $P_p^n[W(a)]$ -LSS. Properties of general LSS hold good for canonical systems. However,

canonical systems have additional properties which are taken up here.

We have seen that when the characteristic matrix A is nonsingular the period of the state cycle is a divisor of period T of the characteristic matrix A . Now we show that in the case of a nonsingular canonical LSS the period of the state cycle which includes the state $x = [0 \ 0 \ \dots \ 1]^T$ is T .

$$\text{Let } A_c = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ a_K & a_{K-1} & & & a_1 \end{bmatrix} \quad (4.1.6)$$

be the characteristic matrix of the canonical system.

The characteristic polynomial of A_c is $F(x) = x^K - \sum_{i=1}^K a_i x^{K-i}$,

which is also equal to its minimal polynomial $m(x)$.

$|A_c| = a_K$ and A_c is nonsingular if a_K is a unit in $P_p^n[W(a)]$ (Section 3.3).

We first prove two lemmas making use of the structure of the matrix A_c .

Lemma 4.1.7

In the matrix A_c^T the elements of the j th row are the coefficients of $x^{\tau+j}$ modulo $[p; m(x)]$, written in the ascending powers of x .

Proof :

Consider matrix A_c as given in Equation (4.1.6). The elements in zeroth row are $[0 \ 1 \ 0 \ \dots \ 0]$ which are coefficients of the polynomial x . The elements in the first row are $[0 \ 0 \ 1 \ \dots \ 0]$ which are the coefficients of the polynomial x^2 . In general the elements in the j th row are the coefficients of the polynomial x^{j+1} , $0 \leq j \leq (K-1)$. The elements of the $(K-1)$ th row are coefficients of polynomial x^K modulo $[p; m(x)]$. That is

$$[a_K \ a_{K-1} \ \dots \ a_3 \ a_2 \ a_1] .$$

Likewise in the matrix,

$$A_c^2 = \begin{bmatrix} 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & & & \vdots \\ a_K & a_{K-1} & & & & a_1 \\ a_1 a_K & & & & & (a_1^2 + a_2) \end{bmatrix}$$

the elements in the zeroth row are coefficients of x^2 , the elements in the first row are coefficients of x^3 , and in general the elements in the j th row are the coefficients of the polynomial x^{j+2} modulo $[p; m(x)]$, $0 \leq j \leq (K-1)$. Thus the elements of the $(K-2)$ th row are the coefficients of the polynomial

$$x^K \text{ modulo } [p; m(x)] .$$

That is

$$[a_K \ a_{K-1} \ \dots \ a_2 \ a_1]$$

and the elements of the $(K-1)$ th row are the coefficients of the polynomial

$$x^{K+1} \text{ modulo}[p; m(x)] .$$

That is

$$[a_1 a_K (a_1 a_{K-1} + a_K) \dots (a_1^2 + a_2)] .$$

In general, in the matrix A_c^τ the elements in the zeroth row are coefficients of $x^\tau \text{ modulo}[p; m(x)]$.

Let $x^\tau = \phi(x) \text{ modulo}[p; m(x)]$; the elements in the first row are coefficients of

$$x^{\tau+1} \text{ modulo}[p; m(x)] = x \phi(x) \text{ modulo}[p; m(x)]$$

Elements in the j th row are the coefficients of $x^{\tau+j} \text{ modulo}[p; m(x)] = x^j \phi(x) \text{ modulo}[p; m(x)]$.

*

Lemma 4.1.8

If the last column of A_c^τ is $[0 \ 0 \ \dots \ 1]^{tr}$ then $A_c^\tau = I$.

Proof :

Elements in the zeroth row of A_c^τ are coefficients of $x^\tau \text{ modulo}[p; m(x)]$.

Let $x^\tau \text{ modulo}[p; m(x)] = \phi(x) = b_K + b_{K-1}x + \dots + b_1x^{K-1}$.

Then the zeroth row of A_C^τ is

$$[b_K \ b_{K-1} \ \dots \ b_2 \ b_1] .$$

From the condition on the last column of A_C^τ , we have $b_1 = 0$.

Hence the elements in the zeroth row of A_C^τ are the coefficients of the polynomial, $\phi(x) = b_K + b_{K-1}x + \dots + b_2x^{K-2}$

Elements in the first row of A_C^τ are the coefficients of the polynomial

$$x\phi(x) \text{ modulo}[p; m(x)] = b_Kx + b_{K-1}x^2 + \dots + b_2x^{K-1}$$

Hence first row of A_C^τ is $[0 \ b_K \ b_{K-1} \ \dots \ b_3b_2]$.

From the condition on the last column of A_C^τ we have $b_2 = 0$.

Hence $x^2\phi(x) \text{ modulo}[p; m(x)] = b_Kx^2 + b_{K-1}x^3 + \dots + b_4x^{K-3} + b_3x^{K-2}$.

Elements in the second row of A_C^τ are the coefficients of $x^2\phi(x) = b_Kx^2 + b_{K-1}x^3 + \dots + b_4x^{K-2} + b_3x^{K-1}$.

Therefore, the second row is $[0 \ 0 \ b_K \ b_{K-1} \ \dots \ b_4 \ b_3]$.

From the condition on the last column of A_C^τ we have $b_3 = 0$.

Hence,

$$x^2\phi(x) = b_Kx^2 + b_{K-1}x^3 + \dots + b_4x^{K-2}$$

Thus we can show that $b_i = 0$; $i = 1, 2, \dots, K-1$ and $(K-1)\text{th}$ row of A_C^τ is $[0 \ 0 \ \dots \ b_K]$.

Since the last column of A_C^τ is $[0 \ 0 \ \dots \ 1]^\tau$ we have $b_K = 1$

and

$$A_C^T = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} = I$$

*

Now we prove the following Theorem.

Theorem 4.1.8

Consider the state $x = (0 \ 0 \ \dots \ 1)^{tr}$ of a nonsingular canonical LSS. Let the period of the characteristic matrix A_C be T . Then the period of the state cycle which contains x is T .

Proof :

Suppose the period of the state cycle which contains x is $\tau \neq T$. Then from Theorem 4.1.1, T is a multiple of τ .

That is, $T = j\tau$; where j is an integer (4.1.7)

We have, $A_C^T x = x$

$$[A_C^T - I]x = 0$$

$$[A_C^T - I] \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Hence the last column of the matrix $[A_C^T - I]$ is equal to $[0 \ 0 \ \dots \ 0]^{tr}$. This implies that the last column of A_C^T is equal to $[0 \ 0 \ \dots \ 1]^{tr}$.

From the result of the Lemma

$$A_C^\tau = I$$

Period of A_C is T . Hence τ is multiple of T . That is,

$$\tau = j'T \quad (4.1.8)$$

From Equation (4.1.7) and (4.1.8) we have $\tau = T$.

Hence the proof. *

Corollary 4.1.3

The state cycle containing the state $x = (0 \ 0 \ \dots \ \alpha)^{tr}$ where α is a unit in $P_p^n[W(a)]$, has a period T ,

Proof :

Let the period of the state cycle containing x be τ .

We have $x = \alpha[0 \ 0 \ \dots \ 1]^{tr}$ and $A_C^\tau x = x$

$$[A_C^\tau - I] = 0$$

$$\alpha [A_C^\tau - I] \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Multiplying by inverse of α on both sides we have,

$$[A_C^\tau - I] \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

From the result of the Theorem 4.1.8 we have

$$\tau = T \quad .$$

*

Example 4.1.8

Consider $A_c = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ over $P_2^2[a^2+1]$. Period of A_c is 6. The state cycle with initial state $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is given below, which has period 6.

$$\begin{pmatrix} 0 & 1 & a & 1+a & a & a \\ 1 & a & 1+a & a & a & 0 \end{pmatrix}$$

The state cycle with initial state $\begin{bmatrix} 0 \\ a \end{bmatrix}$ also has a period 6, as given below

$$\begin{pmatrix} 0 & a & 1 & 1+a & 1 & 1 \\ a & 1 & 1+a & 1 & 1 & 0 \end{pmatrix}$$

*

With respect to the generation of state sequences of maximum possible period, a figure of merit may be defined for any given $P_p^n[W(a)]$ -LSS, which may be used for the sake of comparison of various $P_p^n[W(a)]$ -LSS, as regards to their capability for generating maximum length state sequences.

For a given $P_p^n[W(a)]$ -LSS, the figure of merit denoted by F , may be defined as the ratio of maximum of the periods of state cycles in the state diagram to the total number of nonzero

states. The maximum possible period of a state cycle is T , which is the period of characteristic matrix A and in the case of nonsingular, canonical LSS, there is at least one state cycle of period T . Hence for a K th order $P_p^n[W(a)]$ -LSS,

$$F = \frac{T}{(p^{nK}-1)} .$$

There is no closed form expression for F_{\max} , the maximum value of F . In general, F_{\max} is less than 1, except for the case of $GF(p^n)$ -LSS which have F_{\max} equal to 1. We prove this below.

Theorem 4.1.9

The maximum value of F for a $P_p^n[W(a)]$ -LSS, when $W(a)$ is irreducible is 1.

Proof :

When $W(a)$ is irreducible $P_p^n[W(a)] \simeq GF(p^n)$. Let K be the order of the system. The maximum possible period of A is $(p^{nK}-1)$ and all the $(p^{nK}-1)$ nonzero states lie in a single cycle.

By definition

$$F_{\max} = \frac{(p^{nK}-1)}{(p^{nK}-1)} = 1 .$$

*

Corollary 4.1.4

The maximum value of F for a $P_p^n[W(a)]$ -LSS, where $W(a)$ is not irreducible, is less than 1.

Proof :

From the result of Lemma 4.1.5 and corollary the number of nontrivial state cycles is $> h$. Hence all the nonzero states are not in a single cycle. This implies that the maximum possible period T of state sequence is $< (p^{nK} - 1)$.

Therefore, $F_{\max} < 1$.

*

Lemma 4.1.9

Isomorphic systems have the same F .

Proof

Isomorphic systems have isomorphic state responses. Hence by the definition of F it is same for isomorphic systems.

*

Example 4.1.9

Consider state diagram of $P_2^2[a^2+a]$ -LSS of Example 4.1.3.

$(a^2+a) = a(1+a)$, $h = (2^2-2) = 2$; the two ideals in $P_2^2[a^2+a]$ are $\langle a \rangle = \{0, a\}$.

$\langle 1+a \rangle = \{0, (1+a)\}$.

Number of state cycles with elements from ideals only is 4.

These state cycles are

$$\begin{pmatrix} a & a \\ 0 & a \end{pmatrix} ; \begin{pmatrix} 0 \\ a \end{pmatrix} ; \begin{pmatrix} 0 & 1+a \\ 1+a & 1+a \end{pmatrix} ; \begin{pmatrix} 1+a \\ 0 \end{pmatrix} .$$

There are 15 nonzero states. Period T of matrix A is 2.

Hence, figure of merit $F = 2/15$.

*

Example 4.1.10

Consider state diagram of $P_2^2[a^2+1]$ -LSS with $A = \begin{bmatrix} 1 & 1 \\ a & 1+a \end{bmatrix}$

of Example 4.1.4 ; $(a^2+1) = (a+1)^2$; $h = 3-2 = 1$.

There is only one ideal in $P_2^2[a^2+1]$. This is $\langle a+1 \rangle = \{0, (1+a)\}$

There is only one state cycle with elements from this ideal.

The state cycle is

$$\begin{pmatrix} 1+a & 1+a & 0 \\ 0 & 1+a & 1+a \end{pmatrix}$$

whose period is 3. As seen in Example 4.1.4, there are two more state cycles of length 6. Period T of matrix A is 6. There are 15 nonzero states. Hence figure of merit $F = 6/15$. *

To proceed further we first discuss state isomorphisms.

4.1.5 State Isomorphisms

Isomorphic LSS are discussed in Section 3.6. Two autonomous LSS L and L' defined over isomorphic algebraic structures are isomorphic if there is a one-to-one correspondence between the elements of A and A' and C and C' where A and C correspond to L and A' and C' correspond to L' .

If L and L' are defined over the same algebraic structure say $P_p^n[W(a)]$ as seen in Example 3.6.4 L and L' can be isomorphic if $A' = rA$ and $C' = rC$ where r is a unit in $P_p^n[W(a)]$. For a

state x in L there is a corresponding state $\Theta = rX$ in L' . Also as seen in Example 3.6.5 L and L' can be isomorphic if

$$A' = QAQ^{-1} \quad \text{and} \quad C' = CQ^{-1}$$

where Q is any nonsingular matrix over $P_p^n[W(a)]$. For a state x in L there is a corresponding state $\Theta = Qx$ in L' . Because of the one-to-one correspondence between their states, L and L' have identical or isomorphic state diagrams. Their state response and autonomous response are hence isomorphic. Further from Lemma 4.1.9, they have the same figure of merit.

In the following example we consider the state cycles of $P_2^2[a^2+1]$ -LSS and Z_2^2 -LSS $\simeq P_2^2[a^2+1]$ -LSS and see that the state diagrams are isomorphic.

Example 4.1.11

$$A = \begin{bmatrix} 1 & 1 \\ a & 1+a \end{bmatrix} \quad \text{over} \quad P_2^2[a^2+1]. \quad \text{We obtain the state}$$

cycles using the relation

$$x' = Ax$$

and write the state cycles as a sequence of states given in Table 4.1.2a. Since $|A| = 1$, A is nonsingular.

Table 4.1.2a Sequence of States of $P_2^2[a^2+1]$ -LSS of
Example 4.1.11

Initial state	State sequence	Cycle length
0 0	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	One
a a	$\begin{pmatrix} a & 0 & a & 1 & 0 & 1 \\ a & a & 1+a & 1 & 1 & 1+a \end{pmatrix}$	Six
1 0	$\begin{pmatrix} 1 & 1 & 1+a & a & a & 1+a \\ 0 & a & 1 & 0 & 1 & a \end{pmatrix}$	Six
1+a 1+a	$\begin{pmatrix} 1+a & 0 & 1+a \\ 1+a & 1+a & 0 \end{pmatrix}$	Three

$Z_2^2 \cong P_2^2[a^2+1]$ with the correspondence

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \cong 1; \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \cong a, \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix} \cong (1+a), \quad \begin{bmatrix} 0 \\ 0 \end{bmatrix} \cong 0.$$

The characteristic matrix \bar{A} of isomorphic Z_2^2 -LSS is

$$\bar{A} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

The 2×2 submatrices of \bar{A} are obtained from the correspondence discussed in Section 2.6. We write the state cycles of \mathbb{Z}_2^2 -LSS as a sequence of states given in Table 4.1.2b. The states here are 4-tuples over $\text{GF}(2)$. We use the relation

$$x' = Ax$$

Table 4.1.2b Sequence of States of \mathbb{Z}_2^2 -LSS of Example 4.1.11

Initial state	State sequence	Cycle length
$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	One
$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$	Six
$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$	Six
$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$	Three

From this example it is seen that the two state diagrams are isomorphic. The correspondence between the states in 2nd order $P_2^2[a^2+1]$ -LSS and Z_2^2 -LSS are

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \approx \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \approx \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} a \\ 0 \end{bmatrix} \approx \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ a \end{bmatrix} \approx \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

The other states can be expressed as the linear combination of these over $GF(2)$. Period of A is 6, and Hence $F = \frac{6}{15} = \frac{2}{5}$. The fact that state diagrams of isomorphic $P_p^n[W(a)]$ -LSS, are isomorphic to each other, is utilised in the next section for obtaining the cycle length decomposition of any given $P_p^n[W(a)]$ -LSS in terms of the cycle length decomposition of isomorphic canonical $P_p^n[W(a)]$ -LSS. *

4.2 CYCLE LENGTH DECOMPOSITION OF NONSINGULAR $P_p^n[W(a)]$ -LSS

We have seen that all the states of a nonsingular LSS are cyclic states. Two states x_a and x_b are in the same cycle iff for some j , $x_b = A^j x_a$. x_a and x_b are then said to be A -equivalent. This equivalence relation partitions the set S_x of all states into disjoint classes. Each cycle in the state diagram of a nonsingular autonomous LSS constitutes an equivalence class.

Consider a nonsingular autonomous $P_p^n[W(a)]$ -LSS with μ_i state cycles of length c_i and $\sum_{i=1}^r \mu_i c_i = p^{nK}$. The r -tuple

$$[\mu_1(c_1), \mu_2(c_2), \dots, \mu_r(c_r)] \triangleq \Sigma$$

is called the cycle length decomposition of states of the given LSS. Σ depends on the particular A associated with the system under consideration. Since the autonomous response of LSS is state sequence modified by the matrix C , Σ may be used to obtain all possible periods of output sequences and the number of sequences with these periods. As we have seen in Section 4.1, Σ can also be used to compute the period T of its characteristic matrix A , where $T = \text{lcm}(c_1, c_2, \dots, c_r)$. As we shall see in Section 4.4, when $c = [1 \ 0 \ \dots \ 0]$ Σ can be used to obtain bounds on the number of levels of Hamming correlation functions of output sequences.

Given a nonsingular $P_p^n[W(a)]$ -LSS, Σ can always be obtained by state diagram. However, this procedure is complicated if the order of the system is large. Σ can also be determined, without the state diagram, from the knowledge of the characteristic matrix A of the $P_p^n[W(a)]$ -LSS. The procedure for the determination of Σ of a nonsingular $P_p^n[W(a)]$ -LSS depends on the ring $P_p^n[W(a)]$. When $P_p^n[W(a)]$ is a finite field, the procedure is well established [4,12-14]. When $P_p^n[W(a)]$ is a local ring, the isomorphism between systems and consequently isomorphism between their state diagrams are used to obtain the Σ when $P_p^n[W(a)]$ is a direct sum of primary rings; the Σ is obtained using the decomposition of $P_p^n[W(a)]$ -LSS.

From the characteristic matrix A_1, A_2, \dots of the decomposed subsystems, the cycle length decomposition $\Sigma_1, \Sigma_2, \dots$ of the subsystems are obtained which are then combined to get Σ of $P_p^n[W(a)]$ -LSS.

We have seen in Subsection 4.1.5 that isomorphic systems have isomorphic state diagrams and hence identical cycle length decomposition. Given a system with characteristic matrix A we find an isomorphic system whose cycle length decomposition can be obtained without the help of state diagram. If A is over finite field and if Q is any $K \times K$ nonsingular matrix over the same finite field then QAQ^{-1} and A are similar and give rise to identical cycle length decomposition [4,12-14].

If A is in canonical form its elementary divisor $\lambda(x)$, minimal polynomial $m(x)$ and characteristic polynomial $F(x)$ are same and can be written by inspection. The cycle length decomposition can then be computed in terms of the period of $\lambda(x)$.

When A is in general form we first obtain its elementary divisors (Appendix D). Let the elementary divisors be

$\lambda_1^{h_1}(x), \lambda_2^{h_2}(x), \dots, \lambda_r^{h_r}(x)$, where $\lambda_i(x)$ is irreducible over $GF(p)$; $i = 1, 2, \dots, r$. The form of matrix

$$A_{rc} = \begin{bmatrix} M_{\lambda_1} & & & \\ & M_{\lambda_2} & & \\ & & \ddots & \\ & & & M_{\lambda_r} \end{bmatrix}$$

where M_{λ_i} is the companion matrix of $\lambda_i^{h_i}(x)$, is called the rational canonical form. Further A and A_{rc} are similar [4, 12-14]. Hence the cycle length decomposition with respect to them are identical. A system with characteristic matrix A_{rc} can be assumed to be isomorphic to a combination of systems each having characteristic matrix which is in canonical form and is one of the block matrices in the diagonal of A_{rc} . Σ with respect to A is then computed in terms of the cycle length decomposition with respect to each of the block matrices in A_{rc} .

If $P_p^n[W(a)]$ is a local ring that is, $W(a)$ power of an irreducible polynomial we find characteristic matrix \bar{A} of an isomorphic $GF(p)$ -LSS and obtain the cycle length decomposition by knowing the elementary divisors of \bar{A} over $GF(p)$.

When LSS L is over semisimple or semilocal $P_p^n[W(a)]$, it is decomposed into systems L_1, L_2, \dots, L_r , where system L_i is over $P_p^{h_i n_i}[W_i^{h_i}(a)]$ and has characteristic matrix $A_i = A$ modulo $[p; W_i^{h_i}(a)]$. If $h_i = 1$, A_i is over a field $P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$

and Σ_i can be obtained by computing the elementary divisors of A_i . If $h_i > 1$, A_i is over a local ring and Σ_i can be obtained by considering an isomorphic $\text{GF}(p)$ -LSS with characteristic matrix \bar{A}_i . The Σ of system L is found in terms of $\Sigma_1, \Sigma_2, \dots, \Sigma_y$.

Thus the key concept in obtaining the cycle length decomposition of a nonsingular $P_p^n[W(a)]$ -LSS is to obtain an isomorphic system whose cycle length decomposition can be written without the knowledge of actual state cycles.

In what follows we give the details of the procedure for obtaining Σ of $P_p^n[W(a)]$ -LSS corresponding to the following possible cases.

Case (i) LSS over primary $P_p^n[W(a)]$; $P_p^n[W(a)]$ is a finite field or local ring.

Case (ii) LSS over direct sum of primary rings ; $P_p^n[W(a)]$ is semisimple or semilocal.

4.2.1 LSS over Primary $P_p^n[W(a)]$ Rings

(a) $P_p^n[W(a)]$ is a finite field.

When LSS is over a finite field $P_p^n[W(a)]$, the cycle length decomposition Σ of states of LSS is obtained in a manner similar to the Σ of $\text{GF}(p)$ -LSS, that is from the knowledge of elementary divisors of the characteristic matrix A of the LSS as outlined below. The detail of the procedure for the determination of elementary divisors of A is outlined in Appendix D.

Given A , the matrix $[xI-A]$ is brought to Smith's canonical form, after performing elementary row and column operations. The diagonal elements of the canonical form are field elements or polynomials in x over $GF(p^n)$ and are called invariant factors. The invariant factors are expressed as products of powers of irreducible polynomials over $GF(p^n)$, which are called elementary divisors of the invariant factors. The elementary divisors of all the invariant factors are called elementary divisors of matrix A [12,13,76] when A is in canonical form there is only one invariant polynomial which can be written by inspection. This polynomial is also the characteristic polynomial $F(x)$ of A , defined in Section 3.2.

Cycle length decomposition can be obtained from the knowledge of periods of elementary divisors as explained below. The procedure is similar to the case when A is over finite field $GF(p)$. The determination of periods of polynomials over $GF(p^n)$ is dealt in Appendix D.

Let $\lambda_1(x)$, of degree k_1 be one of the elementary divisors over $P_p^n[W(a)] \simeq GF(p^n)$.

i) if $\lambda_1(x)$ is irreducible and primitive its period is $(p^{nk_1}-1)$ and gives rise to one nontrivial cycle of length $(p^{nk_1}-1)$. This cycle is termed as the maximum length cycle.

ii) if $\lambda_i(x)$ is irreducible over $GF(p^n)$ but not primitive its period T divides $(p^{nk_i}-1)$ and gives rise to $\frac{(p^{nk_i}-1)}{T}$ cycles of length T .

iii) if elementary divisor is $[\lambda_i(x)]^h$ power of an irreducible polynomial over $GF(p^n)$, then let period of $\lambda_i(x)$ be T_{1i} , we find periods.

$$T_{ji} = p^{r_j} T_{1i}$$

where p^{r_j} is the least integer such that $p^{r_j} \geq j$. The cycle length decomposition is then given by

$$\left[1(1), \frac{(p^{nk_1}-1)}{T_{1i}} (T_{1j}), \frac{(p^{2k_1}-p^{nk_1})}{T_{2i}} (T_{2j}), \dots, \frac{(p^{nhk_1}-p^{n(n-1)k_1})}{T_{hi}} \right. \\ \left. \times (T_{hj}) \right] \quad (4.2.1)$$

Suppose,

$$\Sigma_1 = [\mu_{11}(c_{11}), \mu_{12}(c_{12}), \dots, \mu_{1s_1}(c_{1s_1})]$$

and

$$\Sigma_2 = [\mu_{21}(c_{21}), \mu_{22}(c_{22}), \dots, \mu_{2s_2}(c_{2s_2})]$$

be the cycle length decomposition corresponding to elementary divisors $\lambda_1^{h_1}(x)$ and $\lambda_2^{h_2}(x)$ of matrix A . Then the product cycle length decomposition $\Sigma = \Sigma_1 \Sigma_2$ is given by

$$= [\mu_{11}(c_{11}) \mu_{21}(c_{21}), \dots, \mu_{1s_1}(c_{1s_1}) \mu_{2s_2}(c_{2s_2})]$$

product of all pairs of cycle length terms.

Let $\mu_{ij}(c_{ij}) \mu_{lm}(c_{lm})$ be a typical term in the product then

$$\mu_{ij}(c_{ij}) \mu_{lm}(c_{lm}) = \mu_{ij} \mu_{lm} \cdot \gcd(c_{ij}, c_{lm}) (\text{lcm}(c_{ij}, c_{lm})) .$$

In general if $\Sigma_1, \Sigma_2, \dots, \Sigma_r$ are the cycle length decomposition of the r elementary divisors of A , then

$$\Sigma = \Sigma_1 \Sigma_2 \dots \Sigma_r$$

Example 4.2.1

Consider a second order LSS over $P_2^2[a^2+a+1] \simeq GF(2^2)$ whose characteristic matrix is $A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$. The invariant polynomial is (x^2+ax+a) which is primitive over $P_2^2[a^2+a+1] GF(2^2)$. Hence all the nonzero states lie in a cycle of length $(2^2)^2-1 = 15$. The sequence of states over $P_2^2[a^2+a+1]$ is given in Table 4.2.1a.

If the $P_2^2[a^2+a+1]$ -LSS is analysed in terms of isomorphic $GF(2)$ -LSS, then the corresponding characteristic matrix

$$\bar{A} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

where the 2×2 submatrices of \bar{A} are obtained from the elements of A using the correspondence between elements of $P_2^2[a^2+a+1]$ and M_2^2 , ring of matrices $\simeq P_2^2[a^2+a+1]$ given in Section 2.6.

Table 4.2.1a State sequences of $P_2^2[a^2+a+1]$ -LSS of Example 4.2.1

Initial state	State sequence	Cycle length
0 0	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	1
1 0	$\begin{pmatrix} 1 & 0 & a & a^2 & a & a & 0 & a^2 & 1 & a^2 \\ 0 & a & a^2 & a & a & 0 & a^2 & 1 & a^2 & a^2 \\ a^2 & 0 & 1 & a & 1 \\ 0 & 1 & a & 1 & 1 \end{pmatrix}$	15

Table 4.2.1b State Sequences of $GF(2)$ -LSS $\simeq P_2^2[a^2+a+1]$ -LSS of Example 4.2.1

Initial state	State sequence	Cycle length
0 0 0 0	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	1
1 0 0 0	$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	15

The sequence of states with components of states from $GF(2)$ is given in Table 4.2.1b.

A has only one elementary divisor (x^4+x^3+1) over $GF(2)$. This is a primitive polynomial of degree 4 over $GF(2)$. Hence the cycle length decomposition is $[1(1), 1(15)]$.

$$T = 15, (p^{nK}-1) = (2^2)^2-1 = 15. \text{ Hence } F = \frac{15}{15} = 1.$$

*

Example 4.2.2

Consider a second order $P_2^2[a^2+a+1]$ -LSS whose characteristic matrix $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ over $P_2^2[a^2+a+1] \simeq GF(2^2)$. The invariant factor of $[xI-A]$ is (x^2+x+1) over $P_2^2[a^2+a+1]$.

$(x^2+x+1) = (x+a)(x+a^2)$ over $P_2^2[a^2+a+1]$. Hence the elementary divisors of A are $(x+a)$ and $(x+a^2)$. The exponent of $(x+a)$ is 3. Therefore, cycle length decomposition corresponding to elementary divisor $(x+a)$ is $[1(1), 1(3)]$.

The exponent of $(x+a^2)$ is 3. Therefore, cycle length decomposition corresponding to elementary divisor $(x+a^2)$ is $[1(1), 1(3)]$. The cycle length decomposition of states of $P_2^2[a^2+a+1]$ -LSS is

$$[1(1), 1(3)][1(1), 1(3)] = [1(1), 5(3)].$$

The sequence of states over $P_2^2[a^2+a+1]$ is given in Table 4.2.2a.

Table 4.2.2a State Sequences of $P_2^2[a^2+a+1]$ -LSS of Example 4.2.2

$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$;	$\begin{pmatrix} a & 0 & a \\ 0 & a & a \end{pmatrix}$;	$\begin{pmatrix} a^2 & 0 & a^2 \\ 0 & a^2 & a^2 \end{pmatrix}$;
$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$;	$\begin{pmatrix} 1 & a & a^2 \\ a & a^2 & 1 \end{pmatrix}$;	$\begin{pmatrix} a^2 & a & 1 \\ a & 1 & a^2 \end{pmatrix}$	

If we analyse the $P_2^2[a^2+a+1]$ -LSS in terms of isomorphic $GF(2)$ -LSS, then the characteristic matrix A of $GF(2)$ -LSS over $GF(2)$ is a 4×4 matrix.

$$\bar{A} = \begin{bmatrix} 0 & 0 & \vdots & 1 & 0 \\ 0 & 0 & \vdots & 0 & 1 \\ \hline 1 & 0 & \vdots & 1 & 0 \\ 0 & 1 & \vdots & 0 & 1 \end{bmatrix}$$

The 2×2 submatrices of \bar{A} are obtained from elements of A using the correspondence established in Section 2.6.

The sequence of states over $GF(2)$ is given in Table 4.2.2b.

The invariant polynomials of $[xI - \bar{A}]$ are (x^2+x+1) and (x^2+x+1) . Hence the elementary divisors are (x^2+x+1) and (x^2+x+1) . (x^2+x+1) gives rise to a cycle length decomposition

Table 4.2.2b State Sequences of GF(2)-LSS $\cong P_2^2[a^2+a+1]$ -LSS
of Example 4.2.2

$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$;	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$;	$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$;	$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$;
		$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$;	$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$			

Therefore, the cycle length decomposition of states of GF(2)-LSS with the characteristic matrix \bar{A} is

$$[1(1), 1(3)] [1(1), 1(3)] = [1(1), 5(3)] .$$

*

(b) $P_p^n[W(a)]$ is a Local ring :

$$W(a) = W_1^{h_1}(a) ; \text{ where } W_1(a) \text{ is irreducible over } GF(p).$$

Since $P_p^n[W(a)]$ is a ring, the procedure for the determination of cycle length decomposition adopted when $P_p^n[W(a)]$ is a field is not applicable here. This is because division, in general is not permitted in the ring $P_p^n[W(a)]$. However, the cycle length

decomposition can be found from the state diagram or by obtaining elementary divisors of matrix \bar{A} over $\text{GF}(p)$. The state diagrams of $P_p^n[W(a)]$ -LSS with characteristic matrix A and that of $\text{GF}(p)$ -LSS with characteristic matrix \bar{A} are isomorphic.

In the case of finite fields it is possible to have one nontrivial cycle of length $(p^{nK}-1)$ in the state diagram of a $\text{GF}(p^n)$ -LSS. This is not so when the LSS is defined over a ring $P_p^n[W(a)]$.

From the Corollary 4.1.1 it follows that the number of nontrivial cycles in the state diagram is at least (h_1-1) and hence it is not possible to have a state cycle of length $(p^{nK}-1)$. The maximum cycle length that can be obtained is equal to the period of the matrix A , as we have already seen in Subsection 4.1.4. The actual number of cycles and their length are considered here. The procedure is illustrated in the following examples.

Example 4.2.3

Let $A = \begin{bmatrix} 1 & 1 \\ a & 1+a \end{bmatrix}$ over $P_2^2[a^2+1]$. Since A is over a ring the technique of case (i) to obtain cycle length decomposition can not be applied here. Since determinant of A , $|A| = 1$, A is nonsingular. Hence all states are cyclic. The state cycles are enumerated in Example 4.1.11. and the cycle

length decomposition is $[1(1), 1(3), 2(6)]$. Period of A is 6 and $F = 6/15$. The cycle length decomposition can also be obtained by considering the characteristic matrix \bar{A} of an isomorphic $GF(2)$ -LSS. We then have

$$\bar{A} = \begin{bmatrix} 1 & 0 & | & 1 & 0 \\ 0 & 1 & | & 0 & 1 \\ \hline 0 & 1 & | & 1 & 1 \\ 1 & 0 & | & 1 & 1 \end{bmatrix}$$

The elementary divisor of \bar{A} is $(x^2+x+1)^2$ over $GF(2)$. This is square of an irreducible polynomial. The cycle length decomposition is $[1(1), 1(3), 2(6)]$. The state cycles are enumerated as sequence of states in Example 4.1.11. We note here that 12 initial conditions out of 16 give rise to a sequence of length 6. Period T of A is 6 and hence $F=6/15$.

*

Example 4.2.4

Consider the 2nd order LSS of Example 3.4.3 over $P_2^2[a^2+1]$. The characteristic matrix of the system is

$$A = \begin{bmatrix} 1+a & a \\ 1 & 0 \end{bmatrix}$$

Since the elements are from a ring, the technique of case (i) to obtain the cycle length decomposition can not be applied here. The state cycles are given below.

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} a \\ a \end{pmatrix}, \begin{pmatrix} 1+a \\ 1+a \end{pmatrix}$$

$$\begin{pmatrix} 1+a & 0 \\ 0 & 1+a \end{pmatrix}, \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix};$$

$$\begin{pmatrix} 1 & 1+a & a & 0 \\ 0 & 1 & 1+a & a \end{pmatrix}, \begin{pmatrix} a & 1+a & 1 & 0 \\ 0 & a & 1+a & 1 \end{pmatrix}.$$

The cycle length decomposition is

$$[4(1), 2(2), 2(4)]$$

We note here that 8 initial states out of 16 give sequences of length 4. Period T of A is 4 and hence $F = 4/15$. The cycle length decomposition can also be found from the characteristic matrix \bar{A} of an isomorphic $\text{GF}(2)$ -LSS.

$$\bar{A} = \begin{bmatrix} 1 & 1 & \vdots & 0 & 1 \\ 1 & 1 & \vdots & 1 & 0 \\ \hline 1 & 0 & \vdots & 0 & 0 \\ 0 & 1 & \vdots & 0 & 0 \end{bmatrix}$$

as obtained in Example 3.4.3, the elementary divisors of \bar{A} are $(x+1)$, $(x+1)^3$. The cycle length decomposition corresponding to $(x+1)$ is $2(1)$. The cycle length decomposition corresponding to elementary divisor $(x+1)^3$, is obtained using the result

for $GF(2)$ and is $[2(1), 1(2), 1(4)]$. The combined cycle length decomposition Σ of states of LSS is the product of these two

$$\begin{aligned}\Sigma &= 2(1) [2(1), 1(2), 1(4)] \\ &= [4(1), 2(2), 2(4)] .\end{aligned}$$

The state cycles over $GF(2)$ are given below.

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} ; \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} ; \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} ; \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} ; \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} ; \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

We note here that 8 initial states out of 16 give sequences of length 4. Period T of A is 4 and hence $F = 4/15$.

*

We have seen that when A is a $K \times K$ matrix over $P_p^n[W(a)]$ where $W(a)$ is a power of an irreducible polynomial the cycle

length decomposition is obtained in terms of elementary divisors of the $n \times n$ matrix \bar{A} over $GF(p)$. The elementary divisors of \bar{A} are found by reducing the $n \times n$ matrix $[xI - \bar{A}]$ to Smith's canonical form. However, if A itself is in canonical form, the Smith's canonical form of $[xI - A]$ will give the invariant polynomial $x^K - \sum_{i=1}^K a_i x^{K-i}$, where $a_i \in P_p^n[W(a)]$. We obtain the invariant polynomials over $GF(p)$ by replacing a_i by appropriate matrices over $GF(p)$, writing the matrix polynomial as the corresponding polynomial matrix, and performing the elementary row and column operations on the $n \times n$ polynomial matrix. Thus when A is in canonical form we have to handle an $n \times n$ polynomial matrix over $GF(p)$, instead of $n \times n$ polynomial matrix $[xI - \bar{A}]$ where A is a general matrix.

We summarise the procedure below, where A is assumed to be in canonical form.

The minimal polynomial of A can be written by inspection which is

$$m(x) = x^K - \sum_{i=1}^K a_i x^{K-i}$$

where $a_i \in P_p^n[W(a)]$.

To get the cycle length decomposition we make use of the isomorphism between $P_p^n[W(a)] \simeq Z_p^n[W]$. Replacing a_i by appropriate matrices we get the matrix polynomial

$$x^K I - \sum_{i=1}^K \underline{a}_i x^{K-i}$$

where $a_i \in P_p^n[W(a)] \simeq \underline{a}_i \in M_p^n[W]$.

The matrix polynomial is written as a polynomial matrix whose elements are polynomials of degree $\leq K$ over $GF(p)$. By performing elementary row and column operations on this matrix we obtain the invariant polynomials and the elementary divisors over $GF(p)$. Using the results from $GF(p)$ the cycle length decomposition Σ is determined. Since the $P_p^n[W(a)]$ -LSS and $Z_p^n[W]$ -LSS are isomorphic the cycle length decomposition of $P_p^n[W(a)]$ -LSS is also Σ .

Example 4.2.5

Consider $P_2^4[a^4+1]$ -LSS. With $A = \begin{bmatrix} 0 & 1 \\ 1+a+a^2 & a \end{bmatrix}$.

The invariant polynomial of A is $x^2+ax+(1+a+a^2)$ which is also the characteristic polynomial over $P_2^4[a^4+1]$. Using the correspondence

$$a \approx \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The characteristic polynomial of A in matrix polynomial form is

$$x^2 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + x \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

The corresponding polynomial matrix is

$$\begin{bmatrix} x^2+1 & 0 & 1 & x+1 \\ x+1 & x^2+1 & 0 & 1 \\ 1 & x+1 & x^2+1 & 0 \\ 0 & 1 & x+1 & x^2+1 \end{bmatrix}$$

We perform elementary row and column operations to get the invariant polynomial $(x^8+x^4+1) = (x^2+x+1)^4$ and thus the elementary divisor is a power of an irreducible polynomial over $GF(2)$. The cycle length decomposition corresponding to this elementary divisor is

$$[1(1), 1(3), 2(6), 20(12)] .$$

*

4.2.2 LSS Over Direct Sum of Primary $P_p^n[W(a)]$ Rings

(a) $P_p^n[W(a)]$ a semisimple ring; $W(a) = \prod_{i=1}^v W_i(a)$, where $W_i(a)$ are irreducible over $GF(p)$. As seen in Subsection 4.2.1, when $W(a)$ is irreducible over $GF(p)$ if A has one elementary divisor which is primitive over $P_p^n[W(a)]$, then the state diagram has only two cycles; one the trivial cycle and the other of length $(p^{nK}-1)$ contains all the nonzero states. However, when $P_p^n[W(a)]$ is semisimple such case will not arise. It follows from Corollary 4.1.2 that the number of nontrivial cycles in a state diagram is $(2^v - 2)$ and hence it is not possible to have a period $(p^{nK}-1)$. If A is in canonical form, maximum length of

a cycle is T , the period of A . The actual number of cycles and their periods are considered here.

Consider the case $\nu = 2$ that is $W(a) = W_1(a) \cdot W_2(a)$, where $W_1(a)$ and $W_2(a)$ are irreducible polynomials of degree n_1 and n_2 respectively, over $GF(p)$, and obtain relation between state periods.

We have seen in Section 2.4 that

$$P_p^n[W(a)] = J_1 + J_2 \text{ modulo}[p; W(a)]$$

$$\text{and } P_p^n[W(a)] \simeq P_p^{n_1}[W_1(a)] \oplus P_p^{n_2}[W_2(a)]$$

J_1 and J_2 are the ideals generated by orthogonal idempotents in $P_p^n[W(a)]$. Then A can be written as

$$A = A_1 + A_2 \text{ modulo}[p; W(a)]$$

and elements of A_i are from J_i ; $i = 1, 2$,

The set of all states of $P_p^n[W(a)]$ -LSS is a $P_p^n[W(a)]$ -module S_x of rank K . As seen in Section 2.4, when $P_p^n[W(a)]$ is semi-simple the $P_p^n[W(a)]$ -module S_x can be written as the direct sum of $P_p^n[W(a)]$ -submodules S_1, S_2 , where S_i is the set of all K -tuples from J_i , $i = 1, 2$,

That is $S_x = S_1 + S_2$, where the addition is pointwise modulo $[p; W(a)]$.

The cycle length decomposition of $P_p^n[W(a)]$ -module S_x with respect to A depends on the cycle length decomposition of

$P_p^n[W(a)]$ -submodules S_1 and S_2 with respect to A_1 and A_2 respectively. Let $x \in S_x$ be any arbitrary state. Every element in S_x is a unique sum of elements from S_1 and S_2 .

Then $x = x_1 + x_2$ where $x_i \in S_i$; $i = 1, 2$. The least integer c_i such that $A^{c_i} x_i = x_i$ is called the period of the state x_i ; c_i is numerically equal to the length of state cycle containing x_i ; $i = 1, 2$. The period c of x and c_1, c_2 are related. We prove this below.

Lemma 4.2.1

The period c of $x = x_1 + x_2$; $x_i \in S_i$; $i = 1, 2$ is $\text{lcm}(c_1, c_2)$.

Proof :

Let $c' = \text{lcm}(c_1, c_2)$

and period of x be c .

We have seen in Section 3.3 that

$$A^c = A_1^c + A_2^c$$

Hence

$$\begin{aligned} x = A^c x &= A_1^c x_1 + A_2^c x_2 \\ &= x_1 + x_2 \end{aligned}$$

This implies $c_1 | c$ and $c_2 | c$ and c is the least such integer. Hence $c = \text{lcm}(c_1, c_2)$.

Making use of the Lemma 4.2.1, we outline a procedure to obtain the cycle length decomposition of states in S_x in terms of cycle length decomposition of states in S_1 and S_2 . Suppose the cycle length decomposition of S_1 with respect to A_1 is $[1(1), \mu_1(c_1)]$ and that of S_2 with respect to A_2 is $[1(1), \mu_2(c_2)]$ respectively. $\mu_1(c_1)$ denotes μ_1 cycles each of period c_1 . This implies that there are $\mu_1 c_1$ nonzero K -tuples with elements from J_1 that is $\mu_1 c_1$ elements from S_1 , likewise there are $\mu_2 c_2$ nonzero K -tuples with elements from J_2 that is $\mu_2 c_2$ nonzero elements in S_2 . Referring to Section 3.2 we see that c_1 and c_2 can be at most T_1 and T_2 respectively, where T_i is the pseudo period of A_i (Section 3.3), $c_i \nmid T_i$; $i = 1, 2$. As mentioned earlier since every element $x \in S_x$ is a unique sum of $x_1 \in S_1$ and $x_2 \in S_2$, we have $\mu_1 c_1 \mu_2 c_2$ nonzero states in S_x . From the result of the Lemma 4.2.1, every $x \in S_x$, has a period c equal to the $\text{lcm}(c_1 c_2)$. We have $\mu_1 c_1 \mu_2 c_2$ states in S_x each with period c . Hence the number of cycles of states with period c is given by

$$\frac{\mu_1 c_1 \mu_2 c_2}{\text{lcm}(c_1 c_2)} = \frac{\mu_1 \mu_2 c_1 c_2}{\text{lcm}(c_1 c_2)} = \mu_1 \mu_2 \text{gcd}(c_1 c_2) \quad (4.2.2)$$

The cycle length decomposition of all states $x \in S_x$ satisfying the relation (4.2.2) is given by

$$\mu_1 \mu_2 \text{gcd}(c_1, c_2)(c) \quad (4.2.3)$$

Expression (4.2.3) is called the product of two cycle length terms given by

$$[\mu_1(c_1)] [\mu_2(c_2)] = \mu_1 \mu_2 \gcd(c_1, c_2)(c) \quad (4.2.4)$$

The other terms in the cycle length decomposition of S_x with respect to $A \text{ at } 0$ found as follows :

$x = 0$ is in the trivial cycle. This cycle is denoted by $1(1)$

x of the form $x_1 + 0$ gives the cycle length term $\mu_1(c_1)$

x of the form $0 + x_2$ gives the cycle length term $\mu_2(c_2)$.

The product cycle length decomposition of two cycle length decompositions of $[1(1), \mu_1(c_1)]$ and $[1(1), \mu_2(c_2)]$ is thus equal to $[1(1), \mu_1(c_1)] [1(1), \mu_2(c_2)] = [1(1), \mu_1(c_1),$

$$\mu_2(c_2), [\mu_1(c_1)] [\mu_2(c_2)]] .$$

which is equal to all the possible product cycle length terms.

Using relation (4.2.4) we have the cycle length decomposition of S

$$[1(1), \mu_1(c_1)] [1(1), \mu_2(c_2)] = [1(1), \mu_1(c_1), \mu_2(c_2), \mu_1 \mu_2 \gcd(c_1, c_2)(c)] \quad (4.2.5)$$

In general,

$$\text{if } \Sigma_1 = [\mu_{11}(c_{11}), \mu_{12}(c_{12}), \dots, \mu_{1s_1}(c_{1s_1})]$$

$$\text{and } \Sigma_2 = [\mu_{21}(c_{21}), \mu_{22}(c_{22}), \dots, \mu_{2s_2}(c_{2s_2})]$$

are the cycle length decompositions of S_1 with respect to A_1 and

S_2 with respect to A_2 respectively, then the cycle length decomposition Σ of S with respect to A is given by the product $\Sigma_1 \Sigma_2$. The cycle length terms of Σ are all the possible product cycle length terms in Σ_1 and Σ_2

$$\begin{aligned} \Sigma_1 \Sigma_2 = & [\mu_{11}(c_{11}) \mu_{21}(c_{21}), \dots \mu_{11}(c_{11}) \mu_{2s_2}(c_{2s_2}), \\ & \mu_{12}(c_{12}) \mu_{21}(c_{21}), \dots \mu_{12}(c_{12}) \mu_{2s_2}(c_{2s_2}), \\ & \mu_{1s_1}(c_{1s_1}) \mu_{21}(c_{21}), \dots \mu_{1s_1}(c_{1s_1}) \mu_{2s_2}(c_{2s_2})] \end{aligned}$$

In general if $P_p^n[W(a)] = J_1 + J_2 + \dots + J_v$, then
 $A = A_1 + A_2 + \dots + A_v \pmod{p; W(a)}$ and
 and $S_x = S_1 + S_2 + \dots + S_v$

With cycle length decomposition Σ_i of S_i with respect to A_i
 $i = 1, 2, \dots, v$; then the cycle length decomposition of S with respect to A is

$$\Sigma = \Sigma_1 \Sigma_2 \dots \Sigma_v.$$

Example 4.2.6

Consider the ring $P_2^3[a^3+1]$. $P_2^3[a^3+1] = \langle a^2+a+1 \rangle + \langle a^2+a \rangle$,
 where $J_1 = \langle a^2+a+1 \rangle = \{0, 1+a+a^2\}$ and $J_2 = \langle a^2+a \rangle$
 $= \{0, a+a^2, 1+a^2, 1+a\}$. Consider the characteristic matrix

$$A = \begin{bmatrix} 0 & 1 \\ a & 1 \end{bmatrix} \text{ which is in canonical form. We have,}$$

$$1 = (a^2 + a + 1) + (a^2 + a) \text{ modulo}[2; a^3 + 1] \text{ and}$$

$$a = (1 + a + a^2) + (1 + a^2) \text{ modulo}[2; a^3 + 1].$$

S_1 is a module of 2-tuples over J_1 and has 4 elements and S_2 is a module of 2-tuples over J_2 and has 16 elements.

$$A = A_1 + A_2$$

$$= \begin{bmatrix} 0 & 1 + a + a^2 \\ 1 + a + a^2 & 1 + a + a^2 \end{bmatrix} + \begin{bmatrix} 0 & a + a^2 \\ 1 + a^2 & a + a^2 \end{bmatrix} \text{ modulo}[2; a^3 + 1]$$

Cycle length decomposition $[1(1), 1(3)]$ of S_1 with respect to A_1 is given below, in terms of state sequences ;

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 + a + a^2 & 0 & 1 + a + a^2 \\ 0 & 1 + a + a^2 & 1 + a + a^2 \end{pmatrix}$$

Cycle length decomposition $[1(1), 1(15)]$ of S_2 with respect to A_2 is given below in terms of state sequences.

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

$$\begin{pmatrix} a + a^2 & 0 & 1 + a^2 & 1 + a^2 & a + a^2 & 1 + a^2 & 0 & 1 + a & 1 + a \\ 0 & 1 + a^2 & 1 + a^2 & a + a^2 & 1 + a^2 & 0 & 1 + a & 1 + a & 1 + a^2 \\ 1 + a & 1 + a^2 & 1 + a & 0 & a + a^2 & a + a^2 & 1 + a & & \\ 1 + a^2 & 1 + a & 0 & a + a^2 & a + a^2 & 1 + a & a + a^2 & \dots \end{pmatrix}$$

Continuing the example

We see that

$$J_1 = \langle a^2+a+1 \rangle \simeq P_2^1[a+1]$$

and

$$J_2 = \langle a^2+a \rangle \simeq P_2^2[a^2+a+1].$$

Thus product of two nonzero elements in the ideal results in a unique nonzero element.

Hence elementary row and column operations can be performed on

$[x \ e_1(a) \ I-A_1]$ and $[x \ e_2(a) \ I-A_2]$ to get the elementary divisors. Elementary divisor $\lambda_{11}(x)$ of A_1 is

$$\lambda_{11}(x) = (a^2+a+1)x^2 + (a^2+a+1)x + (a^2+a+1) \text{ over } J_1, \text{ where } a^2+a+1 = e_1(a) \in J_1.$$

$$\text{We see that, } (a^2+a+1)x^3 = (a^2+a+1) \text{ modulo}[2; a^3+1]$$

That is, 3 is the least integer such that

$$\lambda_{11}(x) \cdot g(x) = (a^2+a+1)x^3 + (a^2+a+1), \text{ where } g(x) \text{ is a polynomial over } J_1. \text{ We call 3 as the pseudo period of } \lambda_{11}(x).$$

Likewise the elementary divisor $\lambda_{21}(x)$ of A_2 is

$$\lambda_{21}(x) = (a^2+a)x^2 + (a^2+a)x + (a^2+1) \text{ over } J_2.$$

$$\text{We see that } (a^2+a)x^{15} = (a^2+a) \text{ modulo}[2; a^3+1]$$

That is, 15 is the least integer such that

$$\lambda_{21}(x) \cdot g_{21}(x) = (a^2+a)x^{15} + (a^2+a)$$

where $g_{21}(x)$ is a polynomial over J_2 .

We call 15 as the pseudo period of $\lambda_{21}(x)$. We note here that the pseudo periods of A_i and pseudo period of its

minimal polynomial $m_i(x)$ are same ; $i = 1, 2$, The product of cycle length decomposition using (4.2.5) $[1(1), 1(3)]$, $[1(1), 1(15)] = [1(1), 1(3), 1(15), 3(15)] = [1(1), 1(3), 4(15)]$. These cycles are given in Table 4.2.3a. Out of 64 initial states 60 initial states give rise to a sequence of length 15. Period T of A is 15, and number of nonzero states 63. Hence figure of merit $F = 15/63$. The characteristic matrix \bar{A} of isomorphic $GF(2)$ -LSS is

$$\bar{A} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

The 3×3 submatrices are obtained from the elements of A and using the correspondence between elements of $P_p^n[W(a)]$ and $M_p^n[W]$ established in Section 2.6.

The invariant polynomial of \bar{A} over $GF(2)$ is $(x^6 + x^5 + x^4 + x^3 + 1)$. The elementary divisors are $(x^2 + x + 1)$, $(x^4 + x + 1)$.

The cycle length decomposition of states is the product cycle length decomposition

$$[1(1), 1(3)] [1(1), 1(15)] = [1(1), 1(3), 4(15)] .$$

The six cycles are given in Table 4.2.3b.

Table 4.2.3a State Cycles of $P_2^3[a^3+1]$ -LSS of Example 4.2.6

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1+a+a^2 & 1+a+a^2 & 0 \\ 1+a+a^2 & 0 & 1+a+a \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & a & a & a+a^2 & a & 1+a+a^2 & 1+a & a^2 \\ 0 & a & a & a+a^2 & a & 1+a+a^2 & 1+a & a^2 & a \\ & & a & 1+a & 1+a+a^2 & 1 & a+a^2 & a^2 \\ & & & 1+a & 1+a+a^2 & 1 & a+a^2 & a^2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} a & 0 & a^2 & a^2 & 1+a^2 & a^2 & 1+a+a^2 & a+a^2 & 1 \\ 0 & a^2 & a^2 & 1+a^2 & a^2 & 1+a+a^2 & a+a^2 & 1 & a^2 \\ a^2 & a+a^2 & 1+a+a^2 & a & 1+a^2 & 1 \\ a+a^2 & 1+a+a^2 & a & 1+a^2 & 1 & a \end{pmatrix}$$

$$\begin{pmatrix} a^2 & 0 & 1 & 1 & 1+a & 1 & 1+a+a^2 & 1+a^2 & a \\ 0 & 1 & 1 & 1+a & 1 & 1+a+a^2 & 1+a^2 & a & 1 \\ 1 & 1+a^2 & 1+a+a^2 & a^2 & 1+a & a \\ 1+a^2 & 1+a+a^2 & a^2 & 1+a & a & a^2 \end{pmatrix}$$

$$\begin{pmatrix} 1+a & 0 & a+a^2 & a+a^2 & 1+a & a+a^2 & 0 & 1+a^2 & 1+a^2 \\ 0 & a+a^2 & a+a^2 & 1+a & a+a^2 & 0 & 1+a^2 & 1+a^2 & a+a^2 \\ a+a^2 & 1+a^2 & 0 & 1+a & 1+a & 1+a^2 \\ 1+a^2 & 0 & 1+a & 1+a & 1+a^2 & 1+a \end{pmatrix}$$

We note here that there is one to one correspondence between the state cycles of $P_2^3[a^3+1]$ -LSS of order 2 and the isomorphic $GF(2)$ -LSS of order 6. Out of 64 initial states 60 initial state give rise to a sequence of length 15.

We have seen in Section 3.3 that when $P_p^n[W(a)]$ is semi-simple the matrix A can be expressed as the internal direct sum of matrices over ideals generated by orthogonal idempotents in $P_p^n[W(a)]$. Since each of these matrices have elements from the ring $P_p^n[W(a)]$, the cycle length decomposition is obtained by enumeration. However, if we consider the external direct sum of $P_p^n[W(a)]$, each component of the direct summand is a field. A then has external direct sum components $A_1^i, A_2^i, \dots, A_\nu^i$, which are over finite fields. The cycle length decomposition Σ_i^j corresponding to each of the component A_i^j is determined using the results of case (i). Σ is then computed as $\Sigma_1^j \Sigma_2^j \dots \Sigma_\nu^j$.

We have

$$P_p^n[W(a)] \simeq P_p^{n_1}[W_1(a)] \oplus \dots \oplus P_p^{n_\nu}[W_\nu(a)]$$

$W_i(a)$ irreducible polynomial of degree n_i over $GF(p)$.

$$P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$$

Hence $A \simeq [A_1^i, A_2^i, \dots, A_\nu^i]$ where A_i^j is over $P_p^{n_i}[W_i(a)]$,

$i = 1, 2, \dots, \nu$.

The set of all K -tuples over J_i which constitutes the $P_p^n[W(a)]$ -submodule S_i of S is hence isomorphic to the set of all K -tuples over $P_p^{n_i}[W_i(a)]$ which is a $P_p^{n_i}[W_i(a)]$ -submodule S'_i ; $i=1,2, \dots, \nu$.

The cycle length decomposition Σ_i of S_i with respect to A_i is hence equal to the cycle length decomposition Σ'_i of S'_i with respect to A'_i $i = 1,2, \dots, \nu$.

The cycle length decomposition Σ of S with respect to A is equal to $\Sigma = \Sigma_1 \Sigma_2 \dots \Sigma_\nu$

$$= \Sigma'_1 \Sigma'_2 \dots \Sigma'_\nu.$$

The cycle length decomposition of S'_i with respect to A'_i can be determined using the results for the case of finite field $P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$. Foregoing discussion proves the following theorem.

Theorem 4.2.1

$$\text{Let } P_p^n[W(a)] \simeq P_p^{n_1}[W_1(a)] \oplus \dots \oplus P_p^{n_\nu}[W_\nu(a)]$$

where $W_i(a)$; $i = 1,2, \dots, \nu$ are irreducible over $GF(p)$.

The cycle length decomposition of S'_i with respect to A'_i be Σ'_i .

Then cycle length decomposition Σ of S with respect to A is given by

$$\Sigma = \Sigma'_1 \Sigma'_2 \dots \Sigma'_\nu$$

The theorem is illustrated in the following examples.

Example 4.2.7

Consider $A = \begin{bmatrix} 0 & 1 \\ a & 1 \end{bmatrix}$ over $P_2^3[a^3+1] \simeq P_2^1[a+1] \oplus P_2^2[a^2+a+1]$.

A is in canonical form. Hence A_1^1, A_2^1 are also in canonical form.

$$A_1^1 = A \bmod[2; a+1] = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Elementary divisor of A_1^1 is (x^2+x+1) which is primitive over $P_2^1[a+1] \simeq GF(2)$.

Hence, $\Sigma_1^1 = [1(1), 1(3)]$.

$$A_2^1 = A \bmod[2, a^2+a+1] = \begin{bmatrix} 0 & 1 \\ a & 1 \end{bmatrix}$$

Elementary divisor of A_2^1 is (x^2+x+a) which is primitive over $P_2^2[a^2+a+1] \simeq GF(2^2)$. Hence, $\Sigma_2^1 = [1(1), 1(15)]$,

and cycle length decomposition of S with respect to A is

$$\Sigma = \Sigma_1^1 \Sigma_2^1 = [(1), 1(3), 4(15)] .$$

*

Example 4.2.8

Consider the second order $P_2^3[a^3+1]$ -LSS

whose characteristic matrix

$$A = \begin{bmatrix} 0 & 1 \\ a^2 & a+1 \end{bmatrix}$$

$$P_2^3[a^3+1] \simeq P_2^1[a+1] \oplus P_2^2[a^2+a+1]$$

$$A_1^1 = A \bmod(a+1) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Elementary divisor of A_1' is $(x+1)^2$ over $GF(2)$ cycle length decomposition of states with respect to A_1' is $\Sigma_1' = [2(1), 1(2)]$

$$A_2' = A \bmod[a^2+a+1] = \begin{bmatrix} 0 & 1 \\ a+1 & a+1 \end{bmatrix}$$

Elementary divisor of A_2' is $x^2+(a+1)x+(a+1)$. This is primitive polynomial over the field $P_2^2[a^2+a+1]$. Hence cycle length of states with respect to A_2' is $\Sigma_2' = [1(1), 1(15)]$.

Cycle length decomposition Σ of states of LSS with respect to A is

$$\begin{aligned} \Sigma &= \Sigma_1 \Sigma_2 = [2(1), 1(2)] [1(1), 1(15)] \\ &= [2(1), 1(2), 2(15), 1(30)] \end{aligned}$$

The state cycles of length 1,2,15 and 30 respectively are given below.

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} a^2+a+1 \\ a^2+a+1 \end{pmatrix},$$

$$\begin{pmatrix} a^2+a+1 & 0 \\ 0 & a^2+a+1 \end{pmatrix}$$

$$\begin{aligned} \text{i)} \quad & \begin{pmatrix} a^2+a & a^2+a & 0 & a+1 & a^2+1 & a+1 & a+1 & 0 & a^2+1 \\ a^2+a & 0 & a+1 & a^2+1 & a+1 & a+1 & 0 & a^2+1 & a^2+a \\ a^2+a & a^2+1 & a^2+1 & 0 & a^2+a & a+1 & & & \\ a^2+1 & a^2+1 & 0 & a^2+a & a+1 & a^2+a & & & \end{pmatrix} \end{aligned}$$

$$\begin{aligned}
 \text{ii)} \quad & \begin{pmatrix} a^2 & a^2 & a^2+a+1 & a & 1 & a & a \\ a^2 & a^2+a+1 & a & 1 & a & a & a^2+a+1 \\ a^2+a+1 & 1 & a^2 & 1 & 1 & a^2+a+1 & a^2 & a \\ 1 & a^2 & 1 & 1 & a^2+a+1 & a^2 & a & a^2 \end{pmatrix} \\
 & \begin{pmatrix} 1 & 0 & a^2 & a^2+1 & a^2 & a+1 & a^2+a+1 & a^2+1 \\ 0 & a^2 & a^2+1 & a^2 & a+1 & a^2+a+1 & a^2+1 & 1 \\ 1 & a^2+1 & a & 0 & 1 & a+1 & 1 & a^2+a & a^2+a+1 \\ a^2+1 & a & 0 & 1 & a+1 & 1 & a^2+a & a^2+a+1 & a+1 \\ a+1 & a & a+1 & a^2 & 0 & a & a^2+a & a & \\ a & a+1 & a^2 & 0 & a & a^2+a & a & a^2+1 & \\ a^2+1 & a^2+a+1 & a^2+a & a^2 & a^2+a & & & & \\ a^2+a+1 & a^2+a & a^2 & a^2+a & 1 & & & & \end{pmatrix}
 \end{aligned}$$

The characteristic matrix A of an isomorphic $\text{GF}(2)$ -LSS is given below, where the 3×3 submatrices are obtained using the correspondence between elements of matrix A and the matrices M_2^3 established in Section 2.5.

$$\bar{A} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

The elementary divisors of \bar{A} are $(x+1)^2$ and (x^4+x^3+1) over $GF(2)$.

$$\Sigma_1 = [2(1), 1(2)] \text{ corresponding to } (x+1)^2$$

$$\text{and } \Sigma_2 = [1(1), 1(15)] \text{ corresponding to } (x^4+x^3+1).$$

The cycle length decomposition of states of $GF(2)$ -LSS isomorphic to the given $P_2^3[a^3+1]$ -LSS is

$$\Sigma = \Sigma_1 \Sigma_2 = [2(1), 1(2)] [1(1), 1(15)] = [2(1), 1(2), 2(15), 1(30)]$$

We note here that the cycle length decomposition of states of the two isomorphic LSS are same. The state cycles are given below,

State cycles of length 1 are

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

State cycle of length 2 is

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

State cycles of length 15

$$(i) \quad \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$(ii) \quad \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

State cycle of length 30.

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

We note here that the state cycles of $P_2^3[a^3+1]$ -LSS of order 2 have one to one correspondence with the state cycles of isomorphic $GF(2)$ -LSS of order 6.

(b) $P_p^n[W(a)]$ is a semilocal Ring : $W(a) = \prod_{i=1}^v W_i^{h_i}(a)$, where

$W_i(a)$ are distinct irreducible polynomials over $GF(p)$.

As seen in Theorem 2.2.1, the ring $P_p^n[W(a)]$ has

$h = \sum_{i=1}^v [(h_i+1)] - 2$ ideals. Hence from Lemma 4.1.6, in the state diagram of $P_p^n[W(a)]$ -LSS there are at least h nontrivial cycles whose states have components from ideals only. Thus it is not possible to have a state cycle with period $(p^{nK}-1)$. If A is in canonical form the maximum length of a state cycle is equal to the period of A . The determination of cycle length decomposition is taken up below.

We have

$$P_p^n[W(a)] \simeq P_p^{h_1 n_1}[W_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_i n_i}[W_i^{h_i}(a)] \oplus \dots \\ \oplus P_p^{h_v n_v}[W_v^{h_v}(a)]$$

The set S of all states of LSS constitute the $P_p^n[W(a)]$ -module S and

$$S \simeq S'_1 \oplus S'_2 \oplus \dots \oplus S'_v$$

where S'_i is the submodule whose elements have components from

$$P_p^{h_i n_i}[W_i^{h_i}(a)]; \quad i = 1, 2, \dots, v$$

The characteristic matrix,

$$A \approx [A'_1, A'_2, \dots, A'_v]$$

where A'_i has components from $P_p^{h_i n_i}[W_i^{h_i}(a)]$.

Since $P_p^{h_i n_i}[W_i^{h_i}(a)]$ is not a field, the technique used in case (a) for the determination of cycle length decomposition of $S_i^!$ with respect to $A_i^!$ can not be used here. However, cycle length decomposition can be determined by considering the corresponding characteristic matrix $\bar{A}_i^!$ over $GF(p)$. The $h_i n_i \times h_i n_i$ submatrices of $\bar{A}_i^!$ are found using the correspondence between the elements of $A_i^!$ over $P_p^{h_i n_i}[W_i^{h_i}(a)]$ and the $h_i n_i \times h_i n_i$ matrices $\in M_p^{h_i n_i}[W]$ over $GF(p)$, discussed in Section 2.6. The cycle length decomposition Σ_i'' is determined with respect to the $h_i n_i K \times h_i n_i K$ matrix $\bar{A}_i^!$ over $GF(p)$ $i = 1, 2, \dots, \nu$. Then the cycle length decomposition Σ of S with respect to A is given by

$$\Sigma = \Sigma_1'' \Sigma_2'' \dots \Sigma_\nu''$$

The procedure is illustrated in the following examples.

Example 4.2.9

Consider a canonical $P_2^6[a^6+1]$ -LSS with $A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$

$$(a^6+1) = (a+1)^2 (a^2+a+1)^2$$

$$A_1^! = A \text{ modulo}[2; (a+1)^2] = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix} \text{ over local } P_2^2[a^2+1] \text{ ring}$$

$$A_2^! = A \text{ modulo}[2; (a^2+a+1)^2] = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix} \text{ over local } P_2^4[(a^2+a+1)^2] \text{ ring}$$

We use the results of local ring to find Σ_1 and Σ_2 .

To find Σ_1 :

Consider A_1^1

Since A_1^1 is in canonical form the invariant polynomial is x^2+ax+a over $P_2^2[a^2+1]$. The corresponding matrix polynomial

over $GF(2)$ is

$$x^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + x \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and the polynomial matrix is

$$\begin{bmatrix} x^2 & x+1 \\ x+1 & x^2 \end{bmatrix}$$

The elementary divisors of this polynomial matrix is $(x^2+x+1)^2$ over $GF(2)$.

Hence $\Sigma_1 = [1(1), 1(3), 2(6)]$.

To find Σ_2 consider A_2^1 which is in canonical form.

Invariant polynomial of A_2^1 is

$$(x^2+ax+a) \text{ over } P_2^4[(a^2+a+1)^2] .$$

The corresponding matrix polynomial is

$$x^2 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + x \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The corresponding polynomial matrix is

$$\begin{bmatrix} x^2 & 0 & 0 & x+1 \\ x+1 & x^2 & 0 & 0 \\ 0 & x+1 & x^2 & 0 \\ 0 & 0 & x+1 & x^2 \end{bmatrix}$$

The elementary divisor is $(x^4+x+1)^2$

Hence $\Sigma_2 = [1(1), 1(15), 8(30)]$.

Hence cycle length decomposition of states of $P_2^6[a^6+1]$ -LSS is

$$\begin{aligned} \Sigma &= \Sigma_1 \Sigma_2 = [1(1), 1(3), 2(6)] [1(1), 1(15), 8(30)] \\ &= [1(1), 1(3), 2(6), 4(15), 134(30)] . \end{aligned}$$

Out of 4096 initial states, 4020 initial states give a sequence of period 30.

Period T of matrix A from the cycle length decomposition is 30.

Figure of merit F of $P_2^6[a^6+1]$ -LSS is equal to $30/4095$.

4.3 AUTONOMOUS RESPONSE OF $P_p^n[W(a)]$ -LSS

Having studied autonomous state response, we now consider the autonomous response of $P_p^n[W(a)]$ -LSS. Since the autonomous response is a fixed linear transformation of the state response, properties of the autonomous response can be obtained from the properties of the state response considered in the earlier two sections. In what follows, the term LSS means $P_p^n[W(a)]$ -LSS.

We first consider the nature of autonomous response. Since the autonomous response $\{y\}$ with initial state x_0 is

$$\begin{aligned}\{y\} &= (y_0, y_1, \dots) \\ &= (CA^0x_0, CA^1x_0, CA^2x_0, \dots)\end{aligned}$$

it follows that, i) the autonomous response $\{y\}$ of a nilpotent LSS is ultimately a zero sequence, (ii) the autonomous response of a singular (but not nilpotent) LSS is periodic or ultimately periodic depending on the initial state, (iii) the autonomous response of a nonsingular LSS is periodic irrespective of initial states.

The nature of autonomous response, which depends on the nature of A , is summarised in Table 4.3.1. Since autonomous response equals the state sequence modified by the matrix C , properties of state sequences, given in Subsection 4.1.2, carry over to autonomous response. We summarise them below.

- 1) If the initial state x_0 has components from a single ideal J in $P_p^n[W(a)]$, then the elements in the output sequence are from the same ideal.
- 2) Let $P_p^n[W(a)]$ be semisimple and let the elements of A be from an ideal J_1 generated by one of the orthogonal idempotents $e_1(a) \in P_p^n[W(a)]$. Further, let $|A| \neq 0$. Then (i) if the initial state x_0 has components from J_1 , the output sequence is periodic (ii) if the initial state x_0 has components from

Table 4.3.1 Nature of Autonomous Response

Nature of A	Nature of Autonomous response	Remarks
Singular and Nilpotent	All the sequences are ultimately zero	Irrespective of initial state
Singular but not Nilpotent	Sequence may be ultimately zero or ultimately periodic or periodic	Depends on initial state
Nonsingular	All the sequences are periodic	Irrespective of initial state

J_j ; $j \neq i$, then the output sequence is ultimately zero,
 (iii) for arbitrary initial state x_0 , with at least one component a unit in $P_p^n[W(a)]$, the output sequence is ultimately periodic with length of transient equal to 1.

3) Let $P_p^n[W(a)]$ be semilocal and let the elements of A be from an ideal J_i generated by one of the orthogonal idempotents $e_i(a) \in P_p^n[W(a)]$. Then, (i) if $|A|$ is a nilpotent element in J_i , then the output sequence is ultimately periodic or ultimately zero (ii) if $|A|$ is not a nilpotent in J_i and the initial state x_0 has components from J_i , then the output sequence is periodic; if the initial state x_0 has at least one component which is a unit in $P_p^n[W(a)]$, then the output sequence is ultimately periodic with transient of length at most one.

We now consider the relation between the period of the state cycle and the period of autonomous response of a non-singular LSS for a given initial state. First we show that the period of autonomous response $\{y\}$ divides the period T of the characteristic matrix A .

Lemma 4.3.1

The period of the autonomous response $\{y\}$ of a non-singular LSS divides the period T of characteristic matrix A .

Proof

We have $y_N = CA^N x_0$. The period of output sequence $\{y\}$ be k . Then k is the least integer such that, $y_{i+k} = y_i$; for all i .

J_j ; $j \neq i$, then the output sequence is ultimately zero,
 (iii) for arbitrary initial state x_0 , with at least one component a unit in $P_p^n[W(a)]$, the output sequence is ultimately periodic with length of transient equal to 1.

3) Let $P_p^n[W(a)]$ be semilocal and let the elements of A be from an ideal J_i generated by one of the orthogonal idempotents $e_i(a) \in P_p^n[W(a)]$. Then, (i) if $|A|$ is a nilpotent element in J_i , then the output sequence is ultimately periodic or ultimately zero (ii) if $|A|$ is not a nilpotent in J_i and the initial state x_0 has components from J_i , then the output sequence is periodic; if the initial state x_0 has at least one component which is a unit in $P_p^n[W(a)]$, then the output sequence is ultimately periodic with transient of length at most one.

We now consider the relation between the period of the state cycle and the period of autonomous response of a non-singular LSS for a given initial state. First we show that the period of autonomous response $\{y\}$ divides the period T of the characteristic matrix A .

Lemma 4.3.1

The period of the autonomous response $\{y\}$ of a non-singular LSS divides the period T of characteristic matrix A .

Proof

We have $y_N = CA^N x_0$. The period of output sequence $\{y\}$ be k . Then k is the least integer such that, $y_{i+k} = y_i$; for all i

Since T is the period of A , we have

$$CA^{i+T}x_0 = CA^i x_0, \text{ for all } i, \text{ that is } y_{i+T} = y_i, \text{ for all } i$$

Suppose $k \nmid T$ then $T = kq+r$ and $r < k$ and $y_i = y_{i+T} = y_{i+kq+r}$, for all i . Since k is the period of $\{y\}$, this implies

$y_i = y_{i+r}$, for all i . Since $r < k$, this is a contradiction to the assumption that k is the period of $\{y\}$. Therefore, $r = 0$ and $k|T$.

The sequence generated by a nonsingular $P_p^n[W(a)]$ -LSS, thus can have a period atmost T , the period of the characteristic matrix A . We call the sequences of period T generated by $P_p^n[W(a)]$ -LSS as maximum length sequences. For a single output nonsingular canonical LSS with $C = [1 \ 0 \ \dots \ 0]$ we have the following.

Theorem 4.3.1

Let L be a K th order nonsingular canonical single output $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$. If a state $x_0 = [x_0(o), x_1(o), \dots, x_{K-1}(o)]^{tr}$ is in a state cycle of period T_0 , then the autonomous response $\{y\}$, with initial values $y_i = x_i(o)$; $i = 1, 2, \dots, K-1$ will have the same period T_0 .

Proof

Since the period of the state cycle containing the state x_0 is T_0 , the states $x_0, Ax_0, \dots, A^{T_0-1}x_0$ are distinct, and $y_i = C A^i x_0$.

Since $C = [1 \ 0 \ \dots \ 0]$

the sequence

$$y = (y_0, y_1, \dots, y_{K-1}, \dots)$$

is a sequence of first component of states of .

$$x_0, Ax_0, \dots, A^{T_0-1} x_0.$$

Since A is in canonical form the first K components in the sequence y corresponds to the initial state x_0 and the successive K -tuples are the successive states.

Hence,

$$y_i = y_{i+T_0} = y_{i+2T_0} \dots = y_{i+mT_0}.$$

Now we show by contradiction that T_0 is the least integer satisfying the above equalities.

Suppose

$$\begin{aligned} (y_0 \ y_1 \ \dots \ y_{K-1}) &= (y_\tau, y_{\tau+1}, \dots, y_{\tau+K-1}) \\ &= (y_{2\tau}, y_{2\tau+1}, \dots, y_{2\tau+K-1}), \end{aligned}$$

that is, the period of sequence $\{y\}$ is $\tau < T_0$.

Then a K -tuple starting from y_0 and a K -tuple starting from y_τ are identical, which implies that the state sequence $(x_0, Ax_0, \dots, A^{T_0-1} x_0)$ repeats with a period $\tau < T_0$.

This is a contradiction to the assumption that the period of state cycle containing x_0 is T_0 . Hence, the period of the sequence y can not be less than T_0 . We now consider the structure of autonomous response.

The set of all output sequences of a K th order autonomous $GF(p^n)$ -LSS with matrix $C = [1 \ 0 \ \dots \ 0]$, constitutes a vector space of dimension K . For a $P_p^n[W(a)]$ -LSS, we prove the following.

Theorem 4.3.2

The set S_y of all output sequences of a K th order autonomous $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$ is a $P_p^n[W(a)]$ -module.

Proof

We have to show that S_y is an additive abelian group and the following axioms are satisfied.

- i) $b(\{y\} + \{z\}) = b\{y\} + b\{z\}$
- ii) $(b_1 + b_2)\{y\} = b_1\{y\} + b_2\{y\}$
- iii) $b_1 b_2 \{y\} = b_1(b_2 \{y\})$
- iv) $1\{y\} = \{y\}$

where $1, b_1, b_2, b \in P_p^n[W(a)]$, and $\{y\}, \{z\} \in S_y$.

Elements of S_y are sequences over $P_p^n[W(a)]$ which is a commutative ring. Hence, S_y constitutes an abelian group under pointwise addition. Next we show that the sequences in S_y satisfy the module axioms listed above.

i) The N th element of the sequence $\{y\}$ and $\{z\}$ are given by

$$y_N = C A^N x_y ; \quad x_y \text{ is the initial state}$$

$$z_N = C A^N x_z ; \quad x_z \text{ is the initial state}$$

N th element of the sequence $b(\{y\} + \{z\})$ is

$$\begin{aligned} b(\{y\} + \{z\})_N &= b C A^N (x_y + x_z) = b C A^N x_y + b C A^N x_z \\ &= b y_N + b z_N \end{aligned}$$

Hence $b(\{y\} + \{z\}) = (b\{y\}) + (b\{z\})$.

ii) N th element of the sequence $(b_1 + b_2)\{y\}$ is

$$\begin{aligned} (b_1 + b_2)y_N &= (b_1 + b_2) C A^N x_y = b_1 C A^N x_y + b_2 C A^N x_y \\ &= b_1 y_N + b_2 y_N. \end{aligned}$$

Hence, $(b_1 + b_2)\{y\} = b_1\{y\} + b_2\{y\}$.

iii) N th element of the sequence $b_1 b_2 \{y\}$ is

$$\begin{aligned} b_1 b_2 y_N &= b_1 b_2 C A^N x_y = b_1 (b_2 C A^N x_y) \\ &= b_1 (b_2 y_N) \end{aligned}$$

Hence, $b_1 b_2 \{y\} = b_1 (b_2 \{y\})$.

iv) Nth element of the sequence $l\{y\}$ is

$$l.y_N = l.C A^N x_y = C A^N x_y = y_N$$

Hence, $l\{y\} = \{y\}$.

At this stage it is not known whether S_y is a free module in general. For the specific case when A is in canonical form S_y is a free module of rank K as proved in the following theorem.

Theorem 4.3.3

The set S_y of all the output sequences of a single output canonical nonsingular $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$ is a free module of rank K .

Proof

When the single output LSS is canonical, the output sequence corresponding to the initial state x_0 , has the first K components equal to the K components of the state x_0 . That is, each initial state results in a unique output sequence. Any state can be uniquely represented as the linear combination of the following K states. $[1 \ 0 \ \dots \ 0]^{\text{tr}}$, $[0 \ 1 \ \dots \ 0]^{\text{tr}}$, $\dots [0 \ 0 \ \dots \ 1]^{\text{tr}}$.

It, therefore, follows that any output sequence can be expressed as a linear combination of the K output sequences corresponding to the above K states. Hence, S_y has a basis of K sequences and therefore, S_y is a free module of rank K .

*

The number of sequences in S_Y is equal to p^{nK} . These sequences are periodic with period at most equal to T . If we place a window of width T over the p^{nK} sequences belonging to S_Y , we get a new set S_T of p^{nK} sequences of length T .

Let $y = (y_0, y_1, \dots, y_{T-1})$ be a sequence of length T . We denote the cyclic shift of y , by $\sigma_y = (y_{T-1}, y_0, y_1, \dots, y_{T-2})$. In general cyclic shift by τ positions is given by

$$\sigma^\tau y = (y_{T-\tau}, y_{T-\tau+1}, \dots, y_0, \dots, y_{T-\tau-1}) .$$

Now we prove that S_T is closed under cyclic shifts.

Lemma 4.3.2

If $y \in S_T$, then any cyclic shift σ_y^τ of y is also a sequence in S_T .

Proof

$$y = (Cx_y, CAx_y, CA^2x_y, \dots, CA^{T-1}x_y)$$

$$\text{Consider } \sigma y = (CA^{T-1}x_y, Cx_y, \dots, CA^{T-2}x_y)$$

$$= (C(A^{-1}x_y), CA(A^{-1}x_y), \dots, CA^{T-1}(A^{-1}x_y))$$

It is the output sequence generated by the initial value $A^{-1}x_y$ which is also in S_T . Thus in general σ_y^τ is also in S_T .

4.3.1 Autonomous Response of Canonical $P_p^n[W(a)]$ -LSS, Linear Recursion Relations and Linear Recursion Sequences

We show that the autonomous response of a single output

Kth order canonical LSS with $C = [1 \ 0 \ \dots \ 0]$ satisfies a linear recursion relation (LRR) over $P_p^n[W(a)]$ and constitutes a free module of rank K . Hence the autonomous response of these systems may be treated as linear recursion sequence (LRS) over $P_p^n[W(a)]$.

Consider a single output canonical $P_p^n[W(a)]$ -LSS with

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \vdots \\ a_K & a_{K-1} & \dots & a_1 \end{bmatrix} ; a_i \in P_p^n[W(a)], i = 1, 2, \dots, K \quad (4.3.1)$$

$$C = [1 \ 0 \ \dots \ 0],$$

and initial state $x_0 = [x_0(o), \dots, x_{K-1}(o)]^{tr}$; $x_0(o) \in P_p^n[W(a)]$.

The autonomous response of this system is given by

$$y(N) = C A^N x(o) \quad (4.3.2)$$

$$= [1 \ 0 \ \dots \ 0] \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \vdots \\ a_K & a_{K-1} & \dots & a_1 \end{bmatrix}^N \begin{bmatrix} x_0(o) \\ x_1(o) \\ \vdots \\ x_{K-1}(o) \end{bmatrix} \quad (4.3.3)$$

From Equation (4.3.3), we get

$$\begin{aligned}
 y_0 &= [1 \ 0 \ \dots \ 0] \begin{bmatrix} x_0(o) \\ x_1(o) \\ \vdots \\ x_{K-1}(o) \end{bmatrix} = x_0(o) \\
 y_1 &= [1 \ 0 \ \dots \ 0] \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \vdots \\ a_K & a_{K-1} & \dots & a_1 \end{bmatrix} \begin{bmatrix} x_0(o) \\ x_1(o) \\ \vdots \\ x_{K-1}(o) \end{bmatrix} \\
 &= [1 \ 0 \ \dots \ 0] \begin{bmatrix} x_1(o) \\ x_2(o) \\ \vdots \\ x_{K-1}(o) \\ \sum_{i=1}^K a_i x_{K-i}(o) \end{bmatrix} = x_1(o)
 \end{aligned}$$

Defining $\sum_{i=1}^K a_i x_{K-i}(o) = x_K(o)$, it can be shown that,

$$y_i = x_i(o), \quad i = 0, 1, \dots, K-1.$$

Hence we can write $[x_0(o), x_1(o), \dots, x_{K-1}(o)]^{\text{tr}} =$

$$[y_0, y_1, \dots, y_{K-1}]^{\text{tr}} = y^{\text{tr}}.$$

Next we have,

$$y_k = C A^k x(o) = C A^k \begin{bmatrix} x_0(o) \\ x_1(o) \\ \vdots \\ x_{K-1}(o) \end{bmatrix}$$

$$= [1 \ 0 \ \dots \ 0] \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ a_K & a_{K-1} & \dots & a_1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ a_K & a_{K-1} & \dots & a_1 \end{bmatrix}^{K-1} \begin{bmatrix} x_0(o) \\ x_1(o) \\ \vdots \\ x_{K-1}(o) \end{bmatrix}$$

$$= [1 \ 0 \ \dots \ 0] \begin{bmatrix} x_K(o) = \sum_{i=1}^K a_i x_{K-i}(o) \\ x_{K+1}(o) = \sum_{i=1}^K a_i x_{K+1-i}(o) \\ \vdots \\ x_{2K-1}(o) = \sum_{i=1}^K a_i x_{2K-1-i}(o) \end{bmatrix}$$

$$= \sum_{i=1}^K a_i x_{K-i}(o) = \sum_{i=1}^K a_i y_{K-i}$$

Likewise, it can be shown that

$$y_{K+1} = C A^{K+1} y = \sum_{i=1}^K a_i y_{K+1-i}$$

In general, we have

$$y_N = \sum_{i=1}^K a_i y_{N-i} ; \quad N \geq K \quad (4.3.4)$$

Since y_N is a linear combination of immediate past K values. Equation (4.3.4) constitutes a linear recurrence relation, of order K over $P_p^n[W(a)]$, which we denote by $P_p^n[W(a)]$ -LRR. The solution of Equation (4.3.4), which is an infinite sequence, is called a linear recursion sequence (LRS) over $P_p^n[W(a)]$, which we denote by $P_p^n[W(a)]$ -LRS. For the specific case, where $W(a)$ is an irreducible polynomial over $GF(p)$, $P_p^n[W(a)]$ -LRR becomes an LRR over $GF(p^n)$. Therefore, the notion of the $P_p^n[W(a)]$ -LRR, given by (4.3.4), can be seen as a generalisation of LRR over finite fields, such as given in [10,11].

We have seen in Section 2.6 that there is a one-to-one correspondence between the elements of $P_p^n[W(a)]$, $Z_p^n[W]$ and $M_p^n[W]$. With the coefficients a_i and $y_{N-i} \in P_p^n[W(a)]$ in (4.3.4) replaced by appropriate $n \times n$ matrices $M_p^n[W]$ or n -tuples $\in Z_p^n[W]$ we may obtain $M_p^n[W]$ -LRR and $Z_p^n[W]$ -LRR given by

$$\underline{y_N} = \sum_{i=1}^K \underline{a_i} \underline{y_{N-i}} ; \quad \underline{a_i} ; \underline{y_{N-i}} \in M_p^n[W] ; \quad N \geq K \quad (4.3.5)$$

or

$$\underline{y_N} = \sum_{i=1}^K \underline{a_i} \underline{y_{N-i}} \quad \underline{a_i} \in M_p^n[W]$$

$$\underline{y_N} \in Z_p^n[W] ; \quad N \geq K$$

In general, we have

$$y_N = \sum_{i=1}^K a_i y_{N-i} ; N \geq K \quad (4.3.4)$$

Since y_N is a linear combination of immediate past K values. Equation (4.3.4) constitutes a linear recurrence relation, of order K over $P_p^n[W(a)]$, which we denote by $P_p^n[W(a)]$ -LRR. The solution of Equation (4.3.4), which is an infinite sequence, is called a linear recursion sequence (LRS) over $P_p^n[W(a)]$, which we denote by $P_p^n[W(a)]$ -LRS. For the specific case, where $W(a)$ is an irreducible polynomial over $GF(p)$, $P_p^n[W(a)]$ -LRR becomes an LRR over $GF(p^n)$. Therefore, the notion of the $P_p^n[W(a)]$ -LRR, given by (4.3.4), can be seen as a generalisation of LRR over finite fields, such as given in [10,11].

We have seen in Section 2.6 that there is a one-to-one correspondence between the elements of $P_p^n[W(a)]$, $Z_p^n[W]$ and $M_p^n[W]$. With the coefficients a_i and $y_{N-i} \in P_p^n[W(a)]$ in (4.3.4) replaced by appropriate $n \times n$ matrices $M_p^n[W]$ or n -tuples $\in Z_p^n[W]$ we may obtain $M_p^n[W]$ -LRR and $Z_p^n[W]$ -LRR given by

$$\underline{y_N} = \sum_{i=1}^K \underline{a_i} \underline{y_{N-i}} ; \underline{a_i} ; y_{N-i} \in M_p^n[W] ; N \geq K \quad (4.3.5)$$

or

$$\underline{y_N} = \sum_{i=1}^K \underline{a_i} \underline{y_{N-i}} \quad \underline{a_i} \in M_p^n[W]$$

$$y_N \in Z_p^n[W] ; N \geq K$$

The LRS $\{y_N\}$ is an infinite sequence of $n \times n$ matrices $\in M_p^n[W]$ and is a $M_p^n[W]$ -LRS $\simeq P_p^n[W(a)]$ -LRS.

The LRS $\{y_N\}$ is an infinite sequence of n -tuples over $Z_p^n[W]$ and is a $Z_p^n[W]$ -LRS $\simeq P_p^n[W]$ -LRS.

$P_p^n[W(a)]$ -LRS is indeed the output sequence of a single output canonical system. The actual sequence depends on the coefficients a_i of the LRR and the initial values. In other words properties of LRS depends on the matrix A and the initial state.

We have already seen in Section 3.6, that if two LSS are defined over isomorphic structure with one-to-one correspondence between their characterising matrices, with isomorphic initial states, the responses are isomorphic. It follows then, that if $P_p^n[W(a)] \simeq P_p^n[W'(a)]$ and in the K th order $P_p^n[W(a)]$ -LRR $\sum a_i y_{N-i}$ and $P_p^n[W'(a)]$ -LRR $\sum a'_i y'_{N-i}$, where $a_i \simeq a'_i$; $i=1,2,\dots,K$, $y_j \simeq y'_j$; $j = 0,1, \dots, K-1$, then the set of solutions of $P_p^n[W(a)]$ -LRR is isomorphic to the set of solutions of $P_p^n[W'(a)]$ -LRR. Alternatively, we can say that $P_p^n[W(a)]$ -module S is isomorphic to $P_p^n[W'(a)]$ -module S' .

If we have $Z_p^n[W]$ -LRR $\simeq P_p^n[W(a)]$ -LRR, the set of all solutions of $Z_p^n[W]$ -LRR is a set of all sequences of n -tuples over $GF(p)$, isomorphic to the set of all solutions of $P_p^n[W(a)]$ -LRR.

Linear recursion sequences over $P_p^n[W(a)]$ being the autonomous response y of canonical $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$, properties of autonomous state response and output sequence are carried over to the $P_p^n[W(a)]$ -LRS. These are summarised below.

1. The sequences are periodic irrespective of initial values iff a_K is a unit in $P_p^n[W(a)]$. Otherwise the sequences are ultimately periodic or periodic depending on the initial values.
2. The sequences are ultimately zero sequence irrespective of initial values iff all the coefficients a_i ; $i = 1, 2, \dots, K$ are either zero or nilpotent in $P_p^n[W(a)]$.
3. If the initial values are from a single ideal J in $P_p^n[W(a)]$, then the elements in the LRS are from the same ideals.
4. If coefficient a_K is a unit in $P_p^n[W(a)]$, the period of the sequence is a divisor of the period T of the characteristic matrix A . Initial values $y_i = 0$; $i = 0, 1, \dots, K-2$ and $y_{K-1} = \alpha$; where $\alpha \in P_p^n[W(a)]$, is a unit, always generate a sequence with period T .
5. If $P_p^n[W(a)]$ is semisimple and if a_i ; $i = 1, 2, \dots, K$ are elements from an ideal J_i generated by one of the orthogonal idempotents $e_i(a) \in P_p^n[W(a)]$ and $a_K \neq 0$, then ,
 - (i) if the initial values are from J_i , the LRS is periodic;
 - (ii) if the initial values are from J_j ; $j \neq i$, the LRS is ultimately zero ;

- (iii) for arbitrary initial values with atleast one component a unit in $P_p^n[W(a)]$, the LRS is ultimately periodic with length of transient atmost one.
6. If $P_p^n[W(a)]$ is semilocal and if a_i ; $i = 1, 2, \dots K$ are elements from an ideal J_i generated by one of the orthogonal idempotents $e_i(a)$ in $P_p^n[W(a)]$, then, (a) if a_K is a nilpotent in J_i , the LRS is ultimately periodic or ultimately zero, (b) (i) if a_K is not nilpotent in J_i and the initial values are from J_i , the LRS is periodic, (ii) if a_K is not nilpotent in J_i and the initial values are from J_j , $j \neq i$, the LRS is ultimately zero, and (iii) if a_K is not nilpotent in J_i , then for arbitrary initial values with atleast one component a unit in $P_p^n[W(a)]$, the LRS is ultimately periodic with length of transient atmost one.

Solutions of nonsingular $P_p^n[W(a)]$ -LRR of a given order K , which are periodic infinite sequences, with maximum possible period, are the maximum length sequences. In general, for a given $P_p^n[W(a)]$ -LRR of order K , the maximum possible value of the period T is not known. However, if $P_p^n[W(a)] \simeq GF(p^n)$, the maximum value of the period is $(p^{nK}-1)$.

Consider the set S_y of all the solutions of a given $P_p^n[W(a)]$ -LRR. Let the maximum value of the period be T . We place a window of width T over the p^{nK} sequences to get a new

set S_T of p^{nK} sequences of length T . Each sequence in S_T is closed under cyclic shifts. Further, S_T is a free module of rank K .

4.3.2 Generating Functions of Linear Recursion Sequences Over $P_p^n[W(a)]$

In this subsection we rederive some of the properties of $P_p^n[W(a)]$ -LRS in terms of their generating function, as in the case of finite field LRS [11].

Consider infinite sequences,

$$y = (y_0, y_1, \dots) \quad (4.3.6)$$

$$z = (z_0, z_1, \dots) \quad (4.3.7)$$

We define their sum and product respectively as

$$\begin{aligned} y + z &= (y_0, y_1, \dots) + (z_0, z_1, \dots) \\ &= (y_0 + z_0, y_1 + z_1, \dots) \text{ modulo } p, \text{ and} \\ (y_0, y_1, \dots)(z_0, z_1, \dots) &= (v_0, v_1, \dots) \end{aligned}$$

where

$$v_k = \sum_{i+j=k} y_i z_j$$

With these definitions of addition and multiplication, and with $(0, 0, \dots)$ and $(1, 0, \dots)$ as the additive and multiplicative identities, the set of all sequences constitutes a commutative

ring with identity ; the inverse of (y_0, y_1, \dots) is $(-y_0, -y_1, \dots)$ modulo p . The ring contains the element $(0, 1, 0, \dots)$ which we denote by x . From the definition of multiplication we have $x \cdot x = x^2 = (0 \ 1 \ 0 \ \dots)(0 \ 1 \ 0 \ \dots) = (0 \ 0 \ 1 \ 0 \ \dots)$. In general,

$$x^n = (\underbrace{0 \ \dots \ 0}_{n \text{ zeros}} \ 1 \ 0 \ \dots) \text{ for all } n \geq 1$$

If y_i is a single element of the sequence such that

$y_i = (y_i, 0, \dots, 0)$, then we have,

$$x y_i = (0 \ 1 \ 0 \ \dots)(y_i, 0 \ \dots) = y_i \cdot x = (y_i \ 0 \ \dots)(0 \ 1 \ 0 \ \dots) = (0, y_i, 0 \ \dots). \text{ Or in general}$$

$$x^n y_i = (\underbrace{0 \ \dots \ 0}_{n \text{ zeros}}, y_i, 0 \ \dots)$$

Thus x can be regarded as a right shift operator and the sequence y can be written alternatively as

$$(y_0, 0 \ \dots) + (0, y_1, \dots) + (0 \ 0 \ \dots y_i \ 0 \ \dots) + \dots \\ = y_0 + y_1 x + y_2 x^2 + \dots + y_i x^i + \dots$$

The infinite sequence (y_0, y_1, \dots) can therefore be represented by a formal power series in x ,

$$y(x) = \sum_{i=0}^{\infty} y_i x^i \quad (4.3.8)$$

called the generating function of $y = (y_0, y_1, \dots)$

We now show that the generating function of a solution of $P_p^n[W(a)]$ -LRR is a rational function of x .

Consider a K th order $P_p^n[W(a)]$ -LRR given by Equation (4.3.4)

$$y_N = \sum_{i=1}^K a_i y_{N-i}$$

Given the initial values, y_0, y_1, \dots, y_{K-1} , we have the infinite recursion sequence,

$$y = y_0, y_1, y_2, \dots, y_{K-1}, y_K, y_{K+1}, \dots$$

which can be written as

$$y = (y_0, y_1, \dots, y_{K-1}, 0, \dots) + (0 \dots 0, \underbrace{\sum_{i=1}^K a_i y_{K-i}}_{K \text{ zeros}}, \sum_{i=1}^K a_i y_{K+1-i}, \sum_{i=1}^K a_i y_{K+2-i}, \dots)$$

Rearranging terms, we get

$$\begin{aligned} y &= (y_0, y_1, \dots, y_{K-1}, 0 \dots) + \underbrace{a_K (0 \dots 0, y_0, y_1, \dots)}_{K \text{ zeros}} \\ &\quad + \underbrace{a_{K-1} (0 \dots 0, y_1, y_2, \dots)}_{K \text{ zeros}} + \underbrace{a_{K-2} (0 \dots 0, y_2, y_3, \dots)}_{K \text{ zeros}} \\ &\quad + \underbrace{a_1 (0 \dots 0, y_{K-1}, y_K, \dots)}_{K \text{ zeros}} \end{aligned}$$

On the right hand side, except for the first sequence, in all other sequences the first K terms are zero. In the second sequence which is a multiple of a_K , all the terms y_0, y_1, \dots are present. In the third sequence which is a multiple of a_{K-1} , y_0 does not appear. In general, in the $(i+2)$ th sequence which is a multiple of a_K , terms, namely y_0, y_1, \dots, y_{i-1} , do not appear. We add these missing, terms in the sequence and subtract the same. We then have the following,

$$\begin{aligned}
 y &= (y_0, y_1, y_2, \dots, y_{K-1} \ 0 \ 0 \ \dots) \\
 &+ a_K (\underbrace{0 \ \dots \ 0}_{K \text{ zeros}} \ y_0 \ y_1 \ y_2 \ \dots) \\
 &+ a_{K-1} (\underbrace{0 \ \dots \ 0}_{K \text{ zeros}} \ y_0 \ y_1 \ y_2 \ \dots) - a_{K-1} (\underbrace{0 \ 0 \ \dots \ 0}_{(K-1) \text{ zeros}} \ y_0 \ 0 \ \dots) \\
 &+ a_{K-2} (\underbrace{0 \ \dots \ 0}_{K \text{ zeros}} \ y_0 \ y_1 \ \dots) - a_{K-2} (\underbrace{0 \ \dots \ 0}_{(K-2) \text{ zeros}} \ y_0 \ 0 \ \dots) \\
 &\quad - a_{K-2} (\underbrace{0 \ \dots \ 0}_{(K-1) \text{ zeros}} \ y_1 \ 0 \ \dots) \\
 &+ a_1 (0 \ y_0 \ y_1 \ y_2 \ \dots) - a_1 (0 \ y_0 \ 0 \ \dots) - a_1 (0 \ 0 \ y_1 \ 0 \ \dots) \\
 &- a_1 (\underbrace{0 \ \dots \ 0}_{(K-1) \text{ zeros}} \ y_{K-2} \ 0 \ \dots)
 \end{aligned}$$

Rearranging we have,

$$\begin{aligned}
 y &= a_K(0 \dots 0 \ y_0 \ y_1 \ \dots) \\
 &\quad K \text{ zeros} \\
 &+ a_{K-1}(0 \dots 0 \ y_0 \ y_1 \ \dots) \\
 &\quad (K-1) \text{ zeros} \\
 &+ a_{K-2}(0 \dots 0 \ y_0 \ y_1 \ \dots) \\
 &\quad (K-2) \text{ zeros} \\
 &\dots\dots\dots \\
 &+ a_1(0, y_1 \ y_2 \ \dots) \\
 &+ (y_0, 0 \ 0 \ \dots 0) - a_1(0 \ y_0 \ 0 \ \dots) - a_2(0 \ 0 \ y_0 \ 0 \ \dots) \\
 &- a_{K-1}(0 \ \dots \ 0 \ y_0 \ 0 \ \dots) \\
 &\quad (K-1) \text{ zeros} \\
 &+ (0 \ y_1 \ 0 \ \dots) - a_1(0 \ 0 \ y_1 \ 0 \ \dots) - a_2(0 \ 0 \ 0 \ y_1 \ 0 \ \dots) \\
 &\quad - a_{K-2}(0 \ \dots 0, y_1 \ 0 \ \dots) \\
 &\quad K-1 \text{ zeros} \\
 &+ (0 \ 0 \ y_2 \ 0 \ \dots) - a_1(0 \ 0 \ 0 \ y_2 \ 0 \ \dots) - a_2(0 \ 0 \ 0 \ 0 \ y_2 \ 0 \ \dots) \\
 &\quad - a_{K-3}(0 \ 0 \ \dots 0 \ y_2 \ 0 \ \dots) \\
 &\quad K-1 \text{ zeros} \\
 &\dots\dots\dots \\
 &+ (0 \ \dots \ 0 \ y_{K-1} \ 0) \\
 &\quad K-1 \text{ zeros}
 \end{aligned}$$

In terms of operator x we have,

$$\begin{aligned}
 y(x) &= \sum_{i=0}^{\infty} y_i x^i = a_K x^K \sum_{i=0}^{\infty} y_i x^i + a_{K-1} x^{K-1} \sum_{i=0}^{\infty} y_i x^i + \dots \\
 &\quad a_1 x \sum_{i=0}^{\infty} y_i x^i + (1 - a_1 x - a_2 x^2 \dots a_{K-1} x^{K-1}) y_0 \\
 &\quad + (x - a_1 x^2 - a_2 x^3 \dots a_{K-2} x^{K-1}) y_1 \\
 &\quad + (x^2 - a_1 x^3 - a_2 x^4 \dots a_{K-3} x^{K-1}) y_2 \\
 &\quad \vdots \\
 &\quad + x^{K-1} y_{K-1}
 \end{aligned}$$

from which we get

$$\begin{aligned}
 y(x) &= \sum_{i=0}^{\infty} y_i x^i = \\
 &= \frac{[(1 - a_1 x - a_2 x^2 - \dots a_{K-1} x^{K-1}) y_0 + (x - a_1 x^2 - \dots a_{K-2} x^{K-1}) y_1 + (x^2 - a_1 x^3 - \dots a_{K-3} x^{K-1}) y_2 + \dots x^{K-1} y_{K-1}]}{[1 - a_1 x - a_2 x^2 - \dots a_{K-1} x^{K-1} - a_K x^K]} \\
 &= \frac{y_0 + (y_1 - a_1 y_0) x + (y_2 - a_1 y_1 - a_2 y_0) x^2 + \dots + (y_{K-1} - a_1 y_{K-2} - a_2 y_{K-3} - \dots a_{K-1} y_0) x^{K-1}}{[1 - \sum_{i=1}^K a_i x^i]} \\
 &= \frac{u(x)}{[1 - \sum_{i=1}^K a_i x^i]} \quad (4.3.9)
 \end{aligned}$$

The sequence of coefficients of $y(x)$ constitutes the solution of the $P_p^n[W(a)]$ -LRR given by (4.3.4). The polynomial $1 - \sum_{i=1}^K a_i x^i$ has coefficients which are the coefficients of recurrence relation. It is called the characteristic polynomial of the recurrence relation and is denoted by $f(x)$. Since the coefficients of $f(x)$ are the feedback coefficients of the associated canonical single output $P_p^n[W(a)]$ -LSS, we also call $f(x)$ as the feedback polynomial.

In Equation (4.3.9), the numerator polynomial has a degree less than K and depends on the initial values and the coefficients a_i .

Although we have shown $y(x)$ is a rational polynomial, it remains to be shown that $\frac{1}{f(x)}$ is defined. This we show now.

Condition for $f(x)$ to be invertible

The set of all formal power series over a commutative ring is a commutative ring [65,69,71]. $P_p^n[W(a)]$ is a commutative ring. The set of all formal power series over $P_p^n[W(a)]$ hence constitutes a commutative ring which we denote by $P_p^n[W(a)][x]$. Let $h(x) = h_0 + h_1 x + h_2 x^2 + \dots + h_K x^K$ be a polynomial in this ring. The following theorem gives the conditions for $h(x)$ to be a unit in $P_p^n[W(a)][x]$.

Theorem 4.3.4

$h(x)$ is a unit in $P_p^n[W(a)][x]$ iff h_0 is a unit in $P_p^n[W(a)]$.

Proof

Suppose $h(x)$ is a unit in $P_p^n[W(a)][x]$, then there exists a formal power series $g'(x) \in P_p^n[W(a)][x]$ such that

$$h(x).g'(x) = 1$$

$$\text{That is } (h_0 + h_1x + h_2x^2 + \dots) (g'_0 + g'_1x + g'_2x^2 + \dots) = 1$$

Equating coefficients of like powers on both sides we have

$h_0g'_0 = 1$, therefore, $g'_0 = h_0^{-1}$. In general we have,

$\sum_{i=0}^K h_i g'_{K-i} = 0$; for all $K > 0$ which gives the coefficient,

$$g'_K = -h_0^{-1} \left(\sum_{i=1}^K h_i g'_{K-i} \right) ; K > 0 \text{ and } g'_0 = h_0^{-1} \quad (4.3.10)$$

The coefficients $g'_0, g'_1, g'_2 \dots$ of $g'(x)$ are defined if h_0^{-1} is defined, i.e. if h_0 is a unit in $P_p^n[W(a)]$.

On the other hand if h_0 is a unit in $P_p^n[W(a)]$, a polynomial $g(x)$ whose coefficients are given by (4.3.10), can always be found such that

$$h(x).g'(x) = 1$$

Since in the characteristic polynomial

$f(x) = 1 - \sum_{i=1}^K a_i x^i$ of $P_p^n[W(a)]$ -LRR, the constant term is

the identity element, there exists a polynomial $g'(x)$ over $P_p^n[W(a)]$, such that $f(x).g'(x) = 1$.

To proceed further we first give the following definition and Lemma.

Definition 4.3.1

If $\zeta(x)$ is a polynomial of degree K over $P_p^n[W(a)]$, then $x^K \zeta(1/x)$ is called the reciprocal polynomial of $\zeta(x)$.

Lemma 4.3.3

Periods of polynomial $\zeta(x)$ and its reciprocal polynomial are same.

Proof

Let period of $\zeta(x)$ of degree K be T . Then there exists a polynomial $h(x)$ of degree $(T-K)$ such that

$$\zeta(x) h(x) = (x^T - 1)$$

$$\text{then } \zeta\left(\frac{1}{x}\right) h\left(\frac{1}{x}\right) = \left(\frac{1}{x^T} - 1\right) = \frac{(1-x^T)}{x^T}$$

$$x^K \zeta\left(\frac{1}{x}\right) x^{T-K} h\left(\frac{1}{x}\right) = (1-x^T)$$

$$\zeta'(x).h'(x) = (1-x^T) = (-1)(x^T-1)$$

where $\zeta'(x)$ and $h'(x)$ are reciprocal polynomials of $\zeta(x)$ and $h(x)$ respectively. This implies period of $\zeta'(x)$ is T .

Now we prove the following :

Lemma 4.3.4

The characteristic polynomial $F(x)$ of the matrix A and the characteristic polynomial $f(x)$ of the LRR over $P_p^n[W(a)]$, are reciprocal polynomials.

Proof

$$\text{We have } F(x) = x^K - \sum_{i=1}^K a_i x^{K-i}$$

$$x^K F\left(\frac{1}{x}\right) = x^K \left[\frac{1}{x^K} - \sum_{i=1}^K a_i x^{i-K} \right]$$

$$= 1 - \sum_{i=1}^K a_i x^i = f(x) .$$

*

Lemma 4.3.5

The period of $f(x)$ and $F(x)$ over $P_p^n[W(a)]$ are same.

Proof

Since $f(x)$ and $F(x)$ are reciprocal polynomials their periods are same.

Lemmas 4.3.4 and 4.3.5 are used to prove the following:

*

Lemma 4.3.6

If $f(x)$, over semisimple $P_p^n[W(a)]$ is such that $f_i(x) = f(x) \text{ modulo } [p; W_i(a)]$ is primitive over $P_p^{n_i}[W_i(a)]$ $i = 1, 2, \dots, v$, then period of $f(x)$ is $\text{lcm} [(p^{n_1 K} - 1), (p^{n_2 K} - 1), \dots, (p^{n_v K} - 1)]$.

Proof

The period of $f(x)$ and the characteristic matrix A associated with the single output nonsingular $P_p^n[W(a)]$ -LSS are same.

We have $A \approx [\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_\nu]$,

where $\tilde{A}_i = A \text{ modulo}[p; W_i(a)]$.

The period of \tilde{A}_i in canonical form and the characteristic polynomial $\tilde{f}_i(x)$ of LRR, are same. That is

$$\text{period of } \tilde{f}_i(x) = \text{period of } \tilde{A}_i = (p^{n_i K} - 1)$$

$$\begin{aligned} \text{and period of } A &= \text{lcm} [(p^{n_1 K} - 1), (p^{n_2 K} - 1), \dots, (p^{n_\nu K} - 1)] \\ &= \text{period of } f(x). \end{aligned}$$

*

Theorem 4.3.5

Solutions of the $P_p^n[W(a)]$ -LRR

$$y_N = \sum_{i=1}^K a_i y_{N-i} \text{ are periodic sequence iff } a_K \text{ is a}$$

unit in $P_p^n[W(a)]$.

Proof

Suppose a_K is invertible.

From Lemmas 4.3.4 and 4.3.5 there exists a least integer T such that $f(x) | (1-x^T)$. That is, there exists a polynomial $g(x)$ over $P_p^n[W(a)]$ such that $f(x) \cdot g(x) = (1-x^T)$. (4.3.11)

Such a $g(x)$ is unique, for if $\hat{g}(x)$ is also a polynomial such that $f(x) \cdot \hat{g}(x) = (1-x^T)$

$$\text{then } f(x) [g(x) - \hat{g}(x)] = 0$$

$f(x)$ is invertible, therefore, $g(x) - \hat{g}(x) = 0$

$$g(x) = \hat{g}(x) .$$

Referring to Equation (4.3.9), we have $y(x) = \frac{u(x)}{f(x)}$, where $u(x)$ depends on the initial values y_0, y_1, \dots, y_{K-1} and the coefficients a_i ; $i = 1, 2, \dots, K$. Using the Relation (4.3.11) we have

$$y(x) = \frac{u(x) \cdot g(x)}{(1-x^T)} = u(x) \cdot g(x) [1+x^T+x^{2T}+x^{3T}+\dots]$$

Thus when a_K is invertible, $y(x)$ is periodic with period T . The elements in one period of sequence y are given by the coefficients of $u(x) \cdot g(x)$.

Now suppose that the sequence y is periodic with period T . Then $y(x)$ is of the form

$$y(x) = h(x) [1+x^T+x^{2T}+\dots] = \frac{h(x)}{(1-x^T)}$$

From Equation (4.3.9) $y(x) = \frac{u(x)}{f(x)}$; degree of $u(x) < K$.

Therefore, $\frac{h(x)}{(1-x^T)} = \frac{u(x)}{f(x)}$ and $u(x)(1-x^T) = f(x) \cdot h(x)$;

degree of $u(x) < K$. In particular let $y_0 = y_1 = \dots y_{K-2} = 0$ and $y_{K-1} = 1$; then $u(x) = x^{K-1}$ and $f(x) \cdot h(x) = x^{K-1} (1-x^T)$. Since $f(x) \nmid x^{K-1}$ we have $f(x) \mid (1-x^T)$. This implies

$F(x)|(x^T-1)$, where $F(x)$ is characteristic polynomial of A .
Therefore, A is periodic and hence nonsingular which implies
 $|A| = a_K$ is a unit in $P_p^n[W(a)]$.

Theorem 4.3.6

If the period of $f(x)$ is T , then the period of the associated $P_p^n[W(a)]$ -LRS is a divisor of T .

Proof

$$y(x) = \frac{u(x)}{f(x)} = \frac{u(x) \cdot g(x)}{(1-x^T)} = u(x) \cdot g(x) [1+x^T+x^{2T}+\dots]$$

This implies that for all N

$$y_{N+T} = y_N$$

Let k be the period of the sequence $y = (y_0, y_1, \dots)$ then k is the least integer such that for all $N \geq 0$

$$y_{N+k} = y_N.$$

Suppose $k|T$. Then $T = kq+r$; $0 \leq r < k$ and

$y_{N+T} = y_{N+kq+r} = y_{N+r} = y_N$. For all $N \geq 0$. This implies that $r < k$, is the period of the sequence y . This is a contradiction. Hence, $r = 0$ and $T = kq$.

*

Theorem 4.3.7

Let the period of $f(x)$ be T . If the initial conditions $y_0 = y_1 = \dots = y_{k-2} = 0$ and $y_{k-1} = \alpha$ where α is a unit in $P_p^n[W(a)]$, then the period of the sequence $y(x)$ is T .

Proof

We have $u(x) = \alpha x^{K-1}$ and $y(x) = \frac{\alpha x^{K-1}}{f(x)}$; x is not a factor of $f(x)$ and $f(x) = \frac{(1-x^T)}{g(x)}$ and $g(x)$ is of degree $(T-K)$.

$$y(x) = \alpha x^{K-1} g(x) [1+x^T+x^{2T} + \dots]$$

and the sequence has a period T .

*

We now proceed to investigate the correlation properties of sequences over $P_p^n[W(a)]$.

4.4 HAMMING CORRELATION PROPERTIES OF SEQUENCES GENERATED BY AUTONOMOUS $P_p^n[W(a)]$ -LSS

Correlation is one of the important performance measures of sequences, which governs their suitability in practical applications. The definition of correlation between two sequences depends on the application in which the sequences are employed. The conventional definition of correlation functions is based on the inner product (sum of products of the corresponding sequence components). Another definition of correlation is in terms of the Hamming metric [22]. The Hamming correlation between two sequences of equal length is defined as the number of positions in which these sequences have identical symbols [22].

When the sequence elements are from a commutative ring, the product of two elements may result in a zero even if none

of the elements is a zero. In such a situation the Hamming correlation may be more appropriate than the conventional correlation based on the inner product.

To proceed further we give relevant definitions [79].

Definition 4.4.1

A set R of elements is called a metric space if each pair r_1, r_2 in R is assigned a nonnegative number $\rho(r_1, r_2)$ satisfying the following axioms.

1. Identity : $\rho(r_1, r_2) = 0$ iff $r_1 = r_2$
2. Symmetry : $\rho(r_1, r_2) = \rho(r_2, r_1)$
3. Triangle : $\rho(r_1, r_2) + \rho(r_2, r_3) \geq \rho(r_1, r_3)$

$\rho(r_1, r_2)$ is called the metric in R . It is a measure of distance between r_1 and r_2 .

Definition 4.4.2

A linear space R over a field is said to be normed if there is defined in R a numerical valued function $|r|$ which satisfies the following axioms.

1. $|r| \geq 0$
2. $|r| = 0$ iff $r = 0$
3. $|\alpha r| = |\alpha| \cdot |r|$; α is an element of the field.
4. $|r_1 + r_2| \leq |r_1| + |r_2|$ triangle inequality.

The function $|r|$ is called the norm in R . We can also introduce a metric in the normed space R by setting $\rho(r_1, r_2) = |r_1 - r_2|$. The metric axioms are then satisfied.

Definition 4.4.3

A set R of elements r_1, r_2, \dots , is called a normed ring if

- 1) R is a ring
- 2) R is a normed space
- 3) for any two elements $r_1, r_2 \in R$

$$|r_1 r_2| \leq |r_1| |r_2|$$

- 4) If R contains identity e then $|e| = 1$.

Now we show that $P_p^n[W(a)]$ is a metric space. We have seen in Section 2.2 that $P_p^n[W(a)]$ is a linear space, with $\{1, a, \dots, a^{n-1}\}$ as a basis. Let $r(a) \in P_p^n[W(a)]$.

$$\begin{aligned} \text{We define } |r(a)| &= 1 & \text{if } r(a) \neq 0 \in P_p^n[W(a)] \\ |r(a)| &= 0 & \text{if } r(a) = 0 \in P_p^n[W(a)] \end{aligned}$$

Let $\alpha \in GF(p)$.

$$\text{We define } |\alpha| = \begin{cases} 1 & \alpha \text{ is a nonzero element in } GF(p) \\ 0 & \alpha \text{ is the zero element in } GF(p) \end{cases}$$

$$\text{Then } |\alpha r(a)| = |\alpha| \cdot |r(a)|.$$

$P_p^n[W(a)]$ satisfies the axioms of a normed space.

Let $r_1(a), r_2(a) \in P_p^n[W(a)]$. Then $|r_1(a) r_2(a)| \leq |r_1(a)| \cdot |r_2(a)|$ and $|1| = 1$.

$P_p^n[W(a)]$ satisfies the axioms of a normed ring.

We now introduce a metric in the normed space $P_p^n[W(a)]$.
 Let $r_1(a), r_2(a) \in P_p^n[W(a)]$. Then defining $\rho(r_1(a), r_2(a)) \triangleq |r_1(a) - r_2(a)|$, we have

$$\rho(r_1(a), r_2(a)) = \begin{cases} 0 & \text{if } r_1(a) = r_2(a) \\ 1 & \text{if } r_1(a) \neq r_2(a) \end{cases}$$

This metric is called trivial metric

Consider the set S_N of all sequences of length N , over $P_p^n[W(a)]$. S_N is a $P_p^n[W(a)]$ -module, which is free and of rank N . We introduce a metric in S_N .

Let $y = (y_0, y_1, y_2, \dots, y_{N-1})$ and $z = (z_0, z_1, \dots, z_{N-1}) \in S_N$

$$y_i, z_i \in P_p^n[W(a)] .$$

$$\rho(y, z) = |y - z| = \sum_{i=0}^{N-1} \rho(y_i, z_i) = \sum_{i=0}^{N-1} |y_i - z_i|$$

$$\begin{aligned} \text{where } \rho(y_i, z_i) &= 1 && \text{if } y_i \neq z_i \\ &= 0 && \text{if } y_i = z_i \end{aligned}$$

$\rho(y, z)$ is thus the Hamming distance between y and $z \in S_N$

$$\text{and } \rho(y, 0) = |y - 0| = \sum_{i=0}^{N-1} |y_i - 0| = \sum_{i=0}^{N-1} |y_i|$$

is the Hamming weight of y , denoted by W_y .

Remarks 4.4.1

When the sequences are over a finite field, S_N is a vector space. Hamming weight (distance) is then a norm and

hence S_N is a normed space. When S_N is a $P_p^n[W(a)]$ -module, the axiom (3) of normed space namely $|\alpha r| = |\alpha| \cdot |r|$ is not satisfied (Because $\alpha \cdot r$ may be zero $\in S_N$, even though $\alpha \neq 0$, $r \neq 0$). Hence, $P_p^n[W(a)]$ -module S_N is only a metric space. For convenience, we denote $\rho(y, z)$, the Hamming distance between sequences y and z , by D_{yz} .

Example 4.4.1

Let $y = (0, 1, a^2+1, a+1, a^2+a+1, 0)$ be over $P_2^3[a^3+1]$.

Hamming weight W_y of the sequence y is 4.

The Hamming distance between the two sequences can also be interpreted as Hamming weight. For instance

Let $y = (y_0, y_1, \dots, y_{N-1})$

$z = (z_0, z_1, \dots, z_{N-1})$

be two sequences. Consider the sequence

$$y-z = (y_0-z_0, y_1-z_1, \dots, y_{N-1}-z_{N-1})$$

In the sequence $y-z$ whenever $y_i = z_i$, $y_i-z_i = 0$. From the definition of D_{yz} it follows that

$$D_{yz} = W_{y-z} = W_{z-y} \quad (4.4.1)$$

Example 4.4.2

Let $y = (0, 1, a^2+1, a+1, a^2+a+1, 0)$

$z = (1, 0, a^2+1, a^2+a, a^2+a+1, 0)$

be two sequences over $P_2^3[a^3+1]$

$$y-z = (1 \ 1 \ 0 \ a^2+1 \ 0 \ 0)$$

$$W_{y-z} = W_{z-y} = 3$$

$$D_{yz} = 3.$$

The concept of Hamming correlation between two sequences which we take up next, is an extension of the concept of Hamming distance between them. The notion of Hamming distance is used in Chapter 5 in the study of linear codes over $P_p^n[W(a)]$.

4.4.1 Hamming Correlation Functions

If $y = (y_0, y_1, y_2, \dots, y_{N-1})$ is a sequence of length N then the cyclic shift of y is

$$\begin{aligned} \sigma y &= (y_0 \ominus 1, y_1 \ominus 1, y_2 \ominus 1, \dots, y_{(N-1) \ominus 1}) \\ &= (y_{N-1}, y_0, y_1, \dots, y_{N-2}) \end{aligned}$$

$$\begin{aligned} \text{and in general } \sigma^\tau y &= (y_{0 \ominus \tau}, y_{1 \ominus \tau}, \dots, y_{i \ominus \tau}, \dots, y_{(N-1) \ominus \tau}) \\ &= (y_{N-\tau}, y_{N-\tau+1}, \dots, y_0, y_1, \dots, y_{(N-\tau-1)}) \\ &\quad 0 \leq \tau < N, \end{aligned}$$

where the indices are computed modulo N .

Definition 4.4.4

The Hamming cross correlation function $H_{yz}(\tau)$ between two sequences $y = (y_0, y_1, \dots, y_{N-1})$ and $z = (z_0, z_1, \dots, z_{N-1})$ of equal length N over a given alphabet is defined as follows [22].

$$H_{yz}(\tau) = \sum_{i=0}^{N-1} h[y_i, z_{i \ominus \tau}] \quad 0 \leq \tau \leq N-1$$

where \ominus denotes subtraction modulo N and

$$h[y_i, z_j] = \begin{cases} 0 & \text{if } y_i \neq z_j \\ 1 & \text{if } y_i = z_j \end{cases} \quad (4.4.2)$$

For a given τ , the value of Hamming correlation function between two sequences y and z is numerically equal to the number of identical symbols in y and $\sigma^\tau z$, or the number of zeros in $(y - \sigma^\tau z)$.

Let y and z be two sequences of length N . Consider $H_{yz}(\tau)$. By definition,

$$H_{yz}(\tau) = \sum_{i=0}^{N-1} h[y_i, z_{i \ominus \tau}] \quad (4.4.3)$$

which is equal to the number of locations in y and $\sigma^\tau z$ at which the symbols are identical. If we consider the sequence $y - \sigma^\tau z$ the number of nonzero elements in it is equal to the Hamming distance $D_{y, \sigma^\tau y}$ between y and $\sigma^\tau z$, the Hamming correlation function $H_{yz}(\tau)$, which is equal to the number of zeros in $(y - \sigma^\tau z)$, is thus given by

$$H_{yz}(\tau) = (N - D_{y, \sigma^\tau y}) \quad (4.4.4)$$

Example 4.4.3

$$\text{Let } y = (0, 1, 1+a^2, 1+a, 1+a+a^2, 0)$$

and

$$z = (1, 0, 1+a^2, 1+a^2, 1+a+a^2, 0)$$

$H_{yz}(\tau)$ is computed and tabulated, using equations (4.4.3) or (4.4.4).

τ	0	1	2	3	4	5
$H_{yz}(\tau)$	3	2	0	0	1	2

Definition 4.4.5

The Hamming autocorrelation (HACR) function of a sequence $y = (y_0, y_1, \dots, y_{N-1})$ of length N is defined as

$$H_y(\tau) = \sum_{j=0}^{N-1} h[y_j, y_{j \oplus \tau}] \quad \tau = 0, 1, \dots, N-1 \quad (4.4.5)$$

From Equation (4.4.4) we have,

$$H_y(\tau) = (N - D_{y \oplus y}^{\tau}) \quad (4.4.6)$$

In the following example, the computation of H_y is given.

Example 4.4.4

$$\text{Let } y = (0, 1, 1+a^2, 1+a, 1+a+a^2, 0)$$

Using relations (4.4.5) or (4.4.6) we have,

τ	0	1	2	3	4	5
$H_y(\tau)$	6	1	0	0	0	1

In the computation of maximum offpeak value of HACR function or maximum value of HCCR function, the concept of normalised Hamming correlation is useful. The normalised value of HACR or HCCR function is equal to the value of HACR or HCCR function divided by the sequence length.

Example 4.4.5

The normalised values of HCCR function between the sequences y and z of Example 4.4.3 are

τ	0	1	2	3	4	5
Normalised $H_{yz}(\tau)$	$\frac{1}{2}$	$\frac{1}{3}$	0	0	$\frac{1}{6}$	$\frac{1}{3}$

Example 4.4.6

The normalised values of HACR function of sequence y of Example 4.4.4 are,

τ	0	1	2	3	4	5
$H_y(\tau)$	6	1	0	0	0	1

In the computation of maximum offpeak value of HACR function or maximum value of HCCR function, the concept of normalised Hamming correlation is useful. The normalised value of HACR or HCCR function is equal to the value of HACR or HCCR function divided by the sequence length.

Example 4.4.5

The normalised values of HCCR function between the sequences y and z of Example 4.4.3 are

τ	0	1	2	3	4	5
Normalised $H_{yz}(\tau)$	$\frac{1}{2}$	$\frac{1}{3}$	0	0	$\frac{1}{6}$	$\frac{1}{3}$

Example 4.4.6

The normalised values of HACR function of sequence y of Example 4.4.4 are,

τ	0	1	2	3	4	5
Normalised $H_y(\tau)$	1	$\frac{1}{6}$	0	0	0	$\frac{1}{6}$

*

We now consider an example where the sequences are generated by a second order nonsingular, single output $P_2^2[a^2+1]$ -LSS. The HACR function of all the sequences and HCCR function between any two sequences are given in the form of a table.

Example 4.4.7

Consider $P_2^2[a^2+1]$ -LSS of Example 4.1.4 with $A = \begin{bmatrix} 1 & 1 \\ a & 1+a \end{bmatrix}$

and $C = [1 \ 0]$.

Period of A is 6 and cycle length decomposition is $[1(1), 1(3), 2(6)]$.

The output sequences in S_6 are periodic with period which divides 6. They are

$y = (1, 1, 1+a, a, a, 1+a)$ and its cyclic shifts

$z = (a, 0, a, 1, 0, 1)$ and its cyclic shifts

$r = (1+a, 0, 1+a, 1+a, 0, 1+a)$ and its cyclic shifts

and the zero sequence.

The Hamming auto and cross correlation functions are computed and given below.

τ	0	1	2	3	4	5
$H_Y(\tau)$	6	2	0	2	0	2
$H_Z(\tau)$	6	0	2	2	2	0
$H_T(\tau)$	6	2	2	6	2	2
$H_{YZ}(\tau)$	0	2	2	2	2	0
$H_{ZR}(\tau)$	2	0	0	2	0	0
$H_{YR}(\tau)$	2	0	2	2	0	2

Hamming autocorrelation levels are (6,2,0)

Hamming cross correlation levels are (2,0) .

*

We now consider the properties of HACR functions. Let y be a sequence of length N . The HACR function of y has the following properties.

i) $H_Y(\tau) \leq N$

Proof

By definition of $H_Y(\tau)$, its value can be atmost N .

ii) $H_Y(\tau) = H_Y(N-\tau)$ (symmetry property) .

Proof

$$H_Y(\tau) = \sum_{i=1}^{N-1} h[y_i, y_{i \oplus \tau}]$$

$$\text{and } H_Y(N-\tau) = \sum_{i=0}^{N-1} h[y_i, y_{i \oplus (N-\tau)}] = \sum_{i=0}^{N-1} h[y_i, y_{i \oplus \tau}]$$

Let $j = i \oplus \tau$

then $i = j \ominus \tau$

$$\begin{aligned} H_y(N-\tau) &= \sum_{j=0}^{N-1} h[y_{j \ominus \tau}, y_j] \\ &= \sum_{j=0}^{N-1} h[y_j, y_{j \oplus \tau}] = H_y(\tau) \end{aligned}$$

iii) Hamming autocorrelation function value is invariant to cyclic shifts of the sequence.

Proof

Let the sequence y be of length N

$$y = (y_0, y_1, \dots, y_{N-1})$$

and $\sigma_y^t = (y_{N-t}, y_{N-t+1}, \dots, y_{N-1})$

$$H_{\sigma_y^t}(\tau) = \sum_{i=0}^{N-1} h[y_{N-t+i}, y_{(N-t+i) \oplus \tau}]$$

Putting $j = (N-t+i)$ we have

$$H_{\sigma_y^t}(\tau) = \sum_{j=0}^{N-1} h[y_j, y_{j \oplus \tau}] = H_y(\tau)$$

Periodic or cyclic correlation functions of sequences over $GF(p)$ are exhaustively investigated in [10,11,28,29]. Hamming correlation function of family of sequences over Z_p^n is investigated in [23].

4.4.2 Bounds on Values of Hamming Correlation Functions

Consider a nonsingular K th order single output autonomous $P_p^n[W(a)]$ -LSS whose characteristic matrix A is of period T and $C = [1 \ 0 \ \dots \ 0]$. Let S be the set of all p^{nK} output sequences. Sequences in S are infinite periodic sequences whose period divides T . We put a window of width T over S to get a new set S_T of sequences of length T . We have already seen in Subsection 4.3.1 that S_T is a $P_p^n[W(a)]$ -module and is closed under cyclic shift of sequences. We have seen that a metric can be defined on S_T which gives rise to the notion of Hamming distance and Hamming correlation. Since, in general, a closed form expression for the Hamming correlation functions of sequences in S_T can not be given, we are interested in obtaining upper bounds i) on the number of levels in the Hamming autocorrelation (HACR) function of any sequence in S_T , ii) on the number of levels in the Hamming cross correlation (HCCR) function between any two sequences in S_T , iii) on the values of HACR function $H_Y(\tau)$; $\tau \neq 0$, of any sequence $y \in S_T$ and iv) on the values of HCCR function between any two sequences in S_T .

We first obtain a bound on the number of levels of Hamming correlation function values using the cycle length decomposition of states of LSS. We next obtain an improved bound on the number of levels of Hamming correlation function values and

possible values of HACR and HCCR functions using the state diagram. We shall see that the peak value of HCCR function and the maximum value of HACR function for $\tau \neq 0$, can be determined analytically for sequences generated by single output nonsingular canonical $P_p^n[W(a)]$ -LSS under the conditions : i) $P_p^n[W(a)]$ is semisimple and ii) the projection $\tilde{f}_1(x) = f(x) \text{ modulo}[p; W_1(a)]$ of the characteristic polynomial $f(x)$ of the associated LRR on $P_p^{n_1}[W_1(a)]$, $i = 1, 2, \dots, \nu$ is primitive. The possible values of correlation functions can also be determined for sequences generated by second order $P_p^n[W(a)]$ -LSS satisfying the above conditions.

Consider S_T . There are p^{nK} sequences of length T . If y is in S_T , then the cyclic shifts of $y, \sigma y, \sigma^2 y, \dots, \sigma^{T-1} y$ are also in S_T . For such sequence, we have.

Lemma 4.4.1

If y and y' are cyclic shifts of each other, then the set of values of HACR function of each of them is equal to the set of values of HCCR functions between y and y' .

Proof

From the property (iii) of HACR functions, given in previous subsection, a sequence and its cyclic shift will have the same HACR function. Therefore, $H_y(\tau)$ and $H_{y'}(\tau)$ will have the same set of values. y' is a cyclic shift of y . Let $y' = \sigma^{\tau'} y$.

$$H_{yy'}(\tau) = \sum_{i=0}^{T-1} h[y_i, y'_{i \ominus \tau}] = \sum_{i=0}^{T-1} [y_i, y_{i \ominus \tau \ominus \tau'}] = H_y(\tau + \tau')$$

for all τ and τ' , where the indices are computed modulo T . Thus $H_y(\tau)$, $H_{y'}(\tau)$ and $H_{yy'}(\tau)$ have the same set of values.

Thus if y is a sequence in S_T , cyclic shifts, σy , $\sigma^2 y$, ..., $\sigma^{T-1} y$ in S_T have the same correlation levels. Also the number of zeros in a sequence and its cyclic shifts are the same. Hence, cyclic shifts of a sequence y in S_T are not treated as distinct from y .

Consider a subset $S_T^!$ of S_T , such that in $S_T^!$, no sequence is a cyclic shift of any other sequence in $S_T^!$ and any sequence in S_T is either a sequence in $S_T^!$, or its cyclic shift. Then the set $S_T^!$ is called a set of distinct sequences in S_T , and the sequences in $S_T^!$ are called distinct sequences. $S_T^!$ need not be unique.

As we have already seen in the previous subsection, $H_{yz}(\tau)$ is numerically equal to the number of zeros in the sequence $(y - \sigma^\tau z)$. Since S_T is a $P_p^n[W(a)]$ -module which is closed under cyclic shifts, $(y - \sigma^\tau z)$ is also in S_T . It may be either one of the distinct sequences in S_T , or its cyclic shift. Likewise for the computation of the HACR function $H_y(\tau)$, which is numerically equal to the number of zeros in $(y - \sigma^\tau y)$, it is noted that, $(y - \sigma^\tau y)$ is either a distinct sequence in S_T or its cyclic shift. Thus if we know the number of zeros in all the distinct sequences in S_T , possible values of HACR function of any sequence in

S_T and HCCR function between any two sequences in S_T are known.

Theorem 4.4.1

Let the cycle length decomposition of states of a non-singular, single output $P_p^n[W(a)]$ -LSS be $[\mu_1(c_1), \mu_2(c_2), \dots, \mu_r(c_r)]$. Let $\mu = \sum_{i=1}^r \mu_i$. Then the number of levels in the HACR function of any sequence in S_T is atmost μ and the number of levels in the HCCR function between any two distinct sequences in S_T is atmost $(\mu-1)$.

Proof

The state diagram has $\mu = \sum_{i=1}^r \mu_i$ cycles. This implies S_T has μ distinct sequences upto cyclic shifts, including the all zero sequence. The value of HACR function of y , $H_y(\tau)$ is equal to the number of zeros in the sequence $(y - \sigma^\tau y)$, for shifts $\tau = 0, 1, \dots, (T-1)$. Since, $(y - \sigma^\tau y)$ is one of the μ sequences in S_T , $H_y(\tau)$ can have atmost μ values.

Likewise the cross-correlation function value $H_{yz}(\tau)$ between any two distinct sequences y and z , is equal to the number of zeros in the sequence $(y - \sigma^\tau z)$, for shifts $\tau = 0, 1, \dots, (T-1)$. $(y - \sigma^\tau z)$ is one of the $(\mu-1)$ sequences in S_T (zero sequence is excluded). Thus $H_{yz}(\tau)$ can have at most $(\mu-1)$ values.

Example 4.4.8

Consider a second order single output $P_2^2[a^2+1]$ -LSS with

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 1+a \end{bmatrix}. \quad \text{The } \Sigma \text{ of states of this LSS is } [1(1), 1(3), 2(6)].$$

There are three distinct nonzero sequences $\mu = 4$. Hence the number of levels of HACR function ≤ 4 . Number of levels of HCCR function ≤ 3 . As seen in Example 4.4.7 the actual levels are 3 and 2 respectively. *

The above bound on the number of levels of correlation functions is an upper bound. Some of the μ_i sequences of length C_i , $i = 1, 2, \dots, r$ may have same number of zeros, in which case the actual number of correlation levels will be less than that given by Theorem 4.4.1. An improvement in the bound is obtained by utilising the additional information contained in the state diagram.

Consider the state diagram of a nonsingular single output $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$. Let the cycle length decomposition of states of LSS be $[\mu_1(c_1), \mu_2(c_2), \dots, \mu_i(c_i) \dots \mu_r(c_r)]$. There are $\mu = \sum_{i=1}^r \mu_i$ distinct sequences in S_T . Consider $\mu_i(c_i)$. These μ_i cycles of length c_i are classified based on the number of states having their first component equal to zero.

Let $\mu_{i,j}$ cycles of μ_i , have $\eta_{i,j}$ states with their first

component equal to zero. $\eta_{i,j}$ is also equal to the number of zeros in the output sequence of length c_i ; $i = 1, 2, \dots, r$; $j = 1, 2, \dots, j_i$. Thus μ_i state cycles give rise to j_i output sequences with different number of zeros in a periodic length equal to c_i , $i = 1, 2, \dots, r$. Considering sequences of length T , at the most there could be $\sum_{i=1}^r j_i$ sequences with different number of zeros in a period. Hence number of levels in HACR function $\leq \sum_{i=1}^r j_i$ and number of levels in HCCR function $\leq (\sum_{i=1}^r j_i) - 1$; Since $j_i \leq \mu_i \quad \forall i$, this bound is an improved bound.

In S_T , $\mu_{i,j}$ distinct sequences will have $(\eta_{i,j}/c_i) \cdot T$ zeros and the possible values of HACR and HCCR functions are

$$\left\{ \frac{\eta_{1,1} T}{c_1}, \frac{\eta_{1,2} T}{c_2}, \dots, \frac{\eta_{i,j} T}{c_i}, \frac{\eta_{2,1} T}{c_2}, \dots, \frac{\eta_{2,j_2} T}{c_2}, \dots, \right. \\ \left. \frac{\eta_{r,1} T}{c_1}, \frac{\eta_{r,2} T}{c_2}, \dots, \frac{\eta_{r,j_r} T}{c_r} \right\}.$$

Example 4.4.9

Consider the state diagram of $P_2^2[a^2+1]$ -LSS with

$$A = \begin{bmatrix} 1 & 1 \\ a & 1+a \end{bmatrix} \quad \text{and } C = [1 \ 0] \quad \text{of Example 4.4.7. The cycle length decomposition is } 1(1), 1(3), 2(6). \text{ The cycles are}$$

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} ; \begin{pmatrix} 1+a & 0 & 1+a \\ 1+a & 1+a & 0 \end{pmatrix} ;$$

$$\begin{pmatrix} 1 & 1 & 1+a & a & a & 1+a \\ 0 & a & 1 & 0 & 1 & a \end{pmatrix} ; \begin{pmatrix} a & 0 & a & 1 & 0 & 1 \\ a & a & 1+a & 1 & 1 & 1+a \end{pmatrix}$$

Since $C = [1 \ 0]$, S_T consists of sequences of length 6 whose elements are the first component of the states. Here $\mu = 4$. Using the state diagram, we see that the number of zeros in the sequences of length 6 is either 6, or 2 or 0. Number of levels of Hamming autocorrelation function ≤ 3 . Number of levels of Hamming crosscorrelation function ≤ 2 .

From Example 4.4.7, the actual number of levels of HACR function is 3, with values 6, 2 and 0 and the actual number of levels of HCCR function is 2, with values 0 and 2.

*

The value of HACR function $H_y(\tau)$ for $\tau = 0$ of any sequence y is the number of zeros in the sequence $(y-y)$, which is a zero sequence. In finding the maximum value of $H_y(\tau)$, $\tau \neq 0$ or maximum value of HCCR function, it is not necessary to consider the zero sequence or the trivial cycle in the state diagram.

Next we take up the bound on the values of HACR and HCCR functions.

Theorem 4.4.2

Let $[\mu_1(c_1), \dots, \mu_r(c_r)]$ be the cycle length decomposition of states of a nonsingular single output LSS. Let n_j be the maximum number of zeros in sequences of length c_j . Then the maximum value for $\tau \neq 0$ of normalised HACR function or maximum value of HCCR function is

$$\max \text{ of } \left\{ \left[\frac{\eta_2}{c_2}, \frac{\eta_3}{c_3}, \dots, \frac{\eta_r}{c_r} \right] \right\}$$

where the trivial cycle of zero state of length $c_1 = 1$ is excluded.

Proof

The normalised value of HACR function of any sequence in S_T for $\tau = 0$ is 1. For any other shift τ , the normalised value of HACR function of say sequence $y \in S_T$ is equal to the number of zeros in the sequence $(y - \sigma^\tau y)$. Suppose this is a sequence of period c_j , then the number of zeros in $(y - \sigma^\tau y)$ is atmost $\frac{\eta_j}{c_j} T$ and normalised ^{value} of $H_y(\tau)$ is atmost $\frac{\eta_j}{c_j}$. Thus, for $\tau \neq 0$, the value of HACR function of any sequence in S_T is

$\leq \max \left\{ \frac{\eta_2}{c_2}, \frac{\eta_3}{c_3}, \dots, \frac{\eta_r}{c_r} \right\}$. Likewise the value of HCCR function between any two sequences in S_T is $\leq \max \left\{ \frac{\eta_2}{c_2}, \dots, \frac{\eta_j}{c_j} \right\}$.

In the computation of number of levels of correlation functions or the peak values, we have made use of the knowledge of cycle length decomposition of states or the state diagram of

the associated $P_p^n[W(a)]$ -LSS. The bound on the correlation values can be computed analytically for the specific case satisfying the conditions : i) $P_p^n[W(a)]$ is semisimple, ii) the K th order $P_p^n[W(a)]$ -LSS is nonsingular and canonical with characteristic matrix A , such that $\tilde{\Lambda}_i = A$ modulo $[W_i(a)]$ has a period $(p^{n_i K} - 1)$; or in terms of the characteristic polynomial $f(x)$ of the associated LRR, $\tilde{f}_i(x) = f(x)$ modulo $[p; W_i(a)]$ is primitive over $P_p^{n_i}[W_i(a)]$ and has period $(p^{n_i K} - 1)$, $i = 1, 2, \dots, v$.

We consider this case in the following. We make use of the properties of the maximum length sequence over finite fields to obtain the bound analytically. The relevant properties of maximum length (M-L) sequence over finite fields [28] is given first.

Let $GF(p^{n_i})$ be a finite field of order p^{n_i} . Consider an LRR of order K with characteristic polynomial $\tilde{f}_i(x)$ of degree K . Let $\tilde{f}_i(x)$ be primitive over $GF(p^{n_i})$. Then the periodic sequence \tilde{s}_i which is a solution of the given LRR has the following properties.

- i) \tilde{s}_i has maximum possible period $(p^{n_i K} - 1) = N_i$, and hence is a maximum length sequence.
- ii) the number of nonzero elements in \tilde{s}_i is $p^{n_i(K-1)}$ and the number of zeros in the sequence is $(p^{n_i(K-1)} - 1)$,
- iii) \tilde{s}_i has two level HACR $(p^{n_i K} - 1)$ for $\tau = 0$ and $(p^{n_i(K-1)} - 1)$ for all other $\tau \neq 0$,

iv) suppose in the sequence \tilde{s}_i of length $(p^{n_i K} - 1)$, \tilde{s}_i' is a part of the sequence of length $[(p^{n_i K} - 1)/(p^{n_i} - 1)]$ then the sequence \tilde{s}_i is $(\tilde{s}_i', \alpha \tilde{s}_i', \alpha^2 \tilde{s}_i', \dots, \alpha^{p^{n_i} - 2} \tilde{s}_i')$, where α is a primitive element in $GF(p^{n_i})$.

Now we prove the following Lemmas.

Lemma 4.4.2

The output sequence s_i over J_i , where J_i is the ideal generated by orthogonal idempotent $e_i(a)$ in $P_p^n[W(a)]$, is such that $s_i \simeq \tilde{s}_i$; $s_i = e_i(a) \tilde{s}_i$ and has a period $(p^{n_i K} - 1)$, and number of zeros in the sequence is $(p^{n_i(K-1)} - 1)$, $i = 1, 2, \dots, \nu$.

Proof :

$J_i \simeq P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$. As we have seen in Section 2.4, $r_i(a) \in J_i$, $r_i(a) \neq \tilde{r}_i(a) = r_i(a) \text{ modulo } [W_i(a)]$ $P_p^{n_i}[W_i(a)]$ and $r_i(a) = e_i(a) \tilde{r}_i(a)$. Hence, $s_i \simeq \tilde{s}_i = e_i(a) \tilde{s}_i$. \tilde{s}_i is over $P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$, $\tilde{f}_i(x) = f(x) \text{ modulo } [W_i(a)]$ is primitive over $P_p^{n_i}[W_i(a)]$ hence period of \tilde{s}_i and s_i are $(p^{n_i K} - 1)$ and number of zeros in \tilde{s}_i and s_i are $(p^{n_i(K-1)} - 1)$.

Lemma 4.4.3

The sequence s_i over J_i has two level HACR function.

Proof

The proof follows from property iii) and the isomorphism $s_i \simeq \tilde{s}_i$.

Lemma 4.4.4

Let $\tilde{s} = (\tilde{s}_1, \alpha\tilde{s}_1, \alpha^2\tilde{s}_1, \dots, \alpha^{p^n-2}\tilde{s}_1)$ be one period of maximum length sequence over $P_p^n[W(a)] \simeq GF(p^n)$, generated by a K th order single output canonical autonomous $P_p^n[W(a)]$ -LSS. Let $T = (p^{nK}-1)$ and $\Theta = \frac{(p^{nK}-1)}{(p^n-1)}$. Then the Hamming cross-correlation function between \tilde{s} and $\alpha^j\tilde{s} = (\alpha^j\tilde{s}_1, \alpha^{j+1}\tilde{s}_1, \dots, \tilde{s}_1, \alpha\tilde{s}_1, \alpha^{j-1}\tilde{s}_1)$ has two values $(p^{nK}-1)$ for $\tau = j\Theta$ and $(p^{n(K-1)}-1)$ for $\tau \neq j\Theta : 0 \leq j < p^n-1$.

Proof

Since the sequences are shifted version of the same sequence, HCCR function has two levels. We have $\alpha\tilde{s} = (\alpha\tilde{s}_1, \alpha^2\tilde{s}_1, \dots, \alpha^{p^n-2}\tilde{s}_1, \tilde{s}_1)$, where \tilde{s}_1 is a part of the sequence \tilde{s} , whose length is Θ .

By definition, $\alpha\tilde{s} = \sigma^{T-\Theta}\tilde{s}$

$$\text{and } \alpha^j\tilde{s} = \sigma^{T-j\Theta}\tilde{s}$$

Hamming cross-correlation between \tilde{s} and $\alpha^j\tilde{s} = \sigma^{T-j\Theta}\tilde{s}$ will have peak value when the sequences are identical. A shift of $\tau = j\Theta$ in $\alpha^j\tilde{s}$ is $\sigma^{j\Theta}\alpha^j\tilde{s}$ produces sequences \tilde{s} . Hence, peak value $(p^{nK}-1)$ occurs for $\tau = j\Theta$. For $\tau \neq j\Theta$, HCCR function value is $(p^{n(K-1)}-1)$.

The property of M-L sequence proved in Lemma 4.4.4 will be made use of in Section 4.6 for modulation and demodulation of M-L sequences.

The results of the following Lemmas are used to obtain bound on correlation values.

Lemma 4.4.5

Let K and p be positive integers greater than 1. Then $K < p^{K-1} + p^{K-2} + \dots + p + 1$.

Proof

We have to show that $K < p^{K-1} + p^{K-2} + \dots + p + 1 = \frac{(p^K - 1)}{(p - 1)}$.

Or equivalently we have to show

$$p^K > K(p-1) + 1$$

Since $p > 1$. Let $p = (1+q)$, where $q = (p-1)$.

$$(1+q)^K = 1 + Kq + \frac{K(K-1)}{2} q^2 + \dots + q^K = 1 + K(p-1) + Q$$

where $Q > 0$.

Therefore, $p^K > K(p-1) + 1$.

Hence, the inequality is proved.

The inequality is true for all $p > 1$.

Hence is true for p^n also.

We now show that $\frac{(p^{K-1} - 1)}{(p^{K-1} - 1)}$ is a monotonically decreasing function of p .

Lemma 4.4.6

Let $g = \frac{(p^{K-1}-1)}{(p^K-1)}$ where $p > 1$ and $K > 1$, then g is a monotonically decreasing function if dg/dp is negative for all p and $K > 1$.

$$\frac{dg}{dp} = \frac{(p^K-1) [(K-1)p^{K-2}] - [(p^{K-1}-1) K p^{K-1}]}{(p^K-1)^2}$$

The denominator is positive. Hence, dg/dp is negative if the numerator is negative. That is if

$$(K-1)[p^{2K-2} - p^{K-2}] < K[p^{2K-2} - p^{K-1}]$$

$$\text{i.e., if } K[p^{K-1} - p^{K-2}] < p^{2K-2} - p^{K-2}$$

$$\text{if } K < \frac{p^{2K-2} - p^{K-2}}{p^{K-1} - p^{K-2}}$$

$$\text{if } K < \frac{p^{K-1}(p^{K-1} - \frac{1}{p})}{p^{K-1}(1 - \frac{1}{p})}$$

$$\text{if } K < \frac{(p^K - 1)}{(p-1)}$$

$$\text{i.e., if } K < p^{K-1} + p^{K-2} + \dots + 1$$

From the result of the Lemma 4.4.5 this is true. Hence the proof.

Lemma 4.4.7

Let $1 < p_1 < p_2, \dots < p_r,$

$$\text{then max } \left\{ \frac{(p_1^{(K-1)} - 1)}{(p_1 - 1)}, \frac{(p_2^{(K-1)} - 1)}{(p_2 - 1)}, \dots, \frac{(p_{\nu}^{(K-1)} - 1)}{(p_{\nu} - 1)} \right\}$$

$$= \frac{(p_1^{(K-1)} - 1)}{(p_1 - 1)}$$

Proof

$\frac{(p^{(K-1)} - 1)}{(p - 1)}$ is a monotonically decreasing function. The proof follows from the result of Lemma 4.4.6.

Lemma 4.4.8

For $p > 1$ if $p^{n_1} < p^{n_2} \dots < p^{n_{\nu}}$, that is if

$n_1 < n_2 \dots < n_{\nu}$ then

$$\text{max } \left\{ \frac{(p^{n_1(K-1)} - 1)}{(p^{n_1 K} - 1)}, \dots, \frac{(p^{n_{\nu}(K-1)} - 1)}{(p^{n_{\nu} K} - 1)} \right\}$$

$$= \frac{(p^{n_1(K-1)} - 1)}{(p^{n_1 K} - 1)}$$

Proof

Proof follows from the result of Lemma 4.4.7, when p_1 is replaced by p^{n_1} .

*

We now prove the following theorem which provides a bound on correlation values.

Theorem 4.4.3

Consider a K th order nonsingular single output $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$, where $P_p^n[W(a)]$ is semisimple i.e.

$$W(a) = \sum_{i=1}^{\nu} \pi_i W_i(a) ; W_i(a) \text{ is irreducible polynomial of degree}$$

n_i over $GF(p)$ and the characteristic matrix A is such that period of $\tilde{A}_i = A$ modulo $[p; W_i(a)]$ is $(p^{n_i K} - 1)$; $i = 1, 2, \dots, \nu$, and $n_1 < n_i$ for all $i \neq 1$.

Let $T = \text{lcm} [(p^{n_1 K} - 1), (p^{n_2 K} - 1), \dots (p^{n_\nu K} - 1)]$. Then the value of normalised HACR function for $\tau \neq 0$ of any sequence in S_T or the value of normalised HCCR function between any two sequences in S_T is

$$\leq \frac{(p^{n_1(K-1)} - 1)}{(p^{n_1 K} - 1)}$$

Proof

As we have seen in Section 3.3 period of A is

$$T = \text{lcm}[(p^{n_1 K} - 1), (p^{n_2 K} - 1), \dots (p^{n_\nu K} - 1)]$$

S_T is the set of all sequences of length T .

As we have seen in Section 2.4,

$$P_p^n[W(a)] = J_1 + J_2 + \dots + J_\nu$$

$$\simeq P_p^{n_1}[W_1(a)] \oplus \dots \oplus P_p^{n_\nu}[W_\nu(a)]$$

and $J_i \simeq P_p^{n_i}[W_i(a)] ; i = 1, 2, \dots, \nu$.

Any element $r(a) \in P_p^n[W(a)]$ is uniquely represented as

$$r(a) = r_1(a) + r_2(a) + \dots + r_\nu(a),$$

where $r_i(a) = r(a) e_i(a) \in J_i$ $i = 1, 2, \dots, \nu$

and $r(a) = 0 \in P_p^n[W(a)]$ iff $r_i(a) = 0 \in J_i$ for all $i = 1, 2, \dots, \nu$.

$$\text{Hence } S_T = S_1 + S_2 + \dots + S_\nu,$$

where S_i is set of sequences of length T over J_i .

Any sequence $s \in S_T$ can be expressed uniquely as

$$s = s_1 + s_2 + \dots + s_\nu; \quad s_i \in S_i \quad i = 1, 2, \dots, \nu$$

From Lemma 4.4.2 we have

$$s_i \cong \tilde{s}_i; \quad \text{where } \tilde{s}_i \text{ is a sequence over } P_p^{n_i}[W_i(a)].$$

whose period is $(p^{n_i K} - 1) = N_i$.

With number of zeros $(p^{n_i(K-1)} - 1)$ $i = 1, 2, \dots, \nu$.

Number of zeros in length T is $\frac{(p^{n_i(K-1)} - 1) \cdot T}{(p^{n_i K} - 1)} \triangleq \delta_i$

Any element in the sequence s is a zero iff its components in s_1, s_2, \dots, s_ν are zeros. Thus the number of zeros in any sequence s of length $T \in S_T$ can be at most

$$= \max \left\{ \frac{(p^{n_1(K-1)} - 1)T}{(p^{n_1 K} - 1)}, \frac{(p^{n_2(K-1)} - 1)T}{(p^{n_2 K} - 1)}, \dots, \frac{(p^{n_\nu(K-1)} - 1)T}{(p^{n_\nu K} - 1)} \right\}$$

$$= \max \{ \delta_1, \delta_2, \dots, \delta_\nu \} .$$

The value of $H_Y(\tau)$ is the number of zeros in $(y - \sigma_Y^\tau)$ which is a sequence in S_T . Likewise the value of $H_{YZ}(\tau)$ is the number of zeros in $(y - \sigma_Z^\tau)$ which is a sequence in S_T .

Thus the values of normalised HACR function for $\tau \neq 0$ of any sequence and values of normalised HCCR function between any two sequences is $\leq \max \{ \delta_1, \delta_2, \dots, \delta_\nu \}$.

Since $n_1 < n_i$ for all $i \neq 1$.

From the result of the Lemma 4.4.8, we have for $\tau \neq 0$ the normalised value of HACR function and for all τ normalised

$$\text{value of HCCR function} \leq \delta_1 = \frac{(p^{n_1(K-1)} - 1)}{(p^{n_1 K} - 1)} . \quad *$$

If in the above theorem, A is in canonical form, S_T is a set of sequences of length T which are solutions of $P_p^n[W(a)]$ -LRR. The characteristic polynomial $f(x)$ of the LRR then has a period T equal to the period of A . The projections of $f(x)$ on $P_p^{n_i}[W_i(a)]$ that is $\tilde{f}_i(x) = f(x)$ modulo $[p; W_i(a)]$ have periods equal to $(p^{n_i K} - 1)$, which are the maximum possible value. Hence $\tilde{f}_i(x)$ is primitive over $P_p^{n_i}[W_i(a)]$; $i = 1, 2, \dots, \nu$.

Example 4.4.10

Consider the state cycles of Example 4.2.6. The characteristic matrix $A = \begin{bmatrix} 0 & 1 \\ a & 1 \end{bmatrix}$, and the characteristic polynomial of $f(x)$ of the associated LRR is $(1+x+ax^2)$ over $P_2^3[a^3+1]$. $\tilde{f}_1(x) = (1+x+ax^2) \text{ modulo}[2; a+1] = (1+x+x^2)$ and is primitive over $P_2^1[a+1]$, $\tilde{f}_2(x) = (1+x+ax^2) \text{ modulo}[2; a^2+a+1] = (1+x+ax^2)$ and is primitive over $P_2^2[a^2+a+1]$. Period of $\tilde{f}_1(x)$ $(2^2-1) = 3$. Hence the period of sequence \tilde{s}_1 (modulo[2; $a+1$]) is 3 and number of zeros in this sequence is 1. Period of $\tilde{f}_2(x)$ is $(4^2-1) = 15$. Hence the period of sequence \tilde{s}_2 (modulo[2; a^2+a+1]) is 15 and number of zeros in this sequence is $(4-1) = 3$. Thus, the values of normalised HACR function for $\tau \neq 0$ of any sequence and values of normalised HCCR function between any two sequences is $\leq \max \left\{ \frac{1}{3}, \frac{1}{5} \right\}$.

Set S_1 of sequences over $J_1 = \langle a^2+a+1 \rangle$ consists of sequence $s_1 = (1+a+a^2, 0, 1+a+a^2, 1+a+a^2, \dots)$ and its cyclic shifts. Likewise set S_2 of sequences over $J_2 = \langle a^2+a \rangle$ consists of sequence $s_2 = ((a+a^2), 0, (1+a^2), (1+a^2), (a+a^2), (1+a^2), 0, (1+a), (1+a), (1+a^2), (1+a), 0, (a+a^2), (a+a^2), (1+a), (a+a^2), 0, (1+a^2), \dots)$ and its cyclic shifts. Any solution of $P_2^3[a^3+1]$ -LRR with $f(x) = 1+x+ax^2$ is a linear combination over $P_2^3[a^3+1]$ of the sequences from S_1 and S_2 . It is of the form $(\alpha_1 \sigma^{\tau_1} s_1 + \alpha_2 \sigma^{\tau_2} s_2)$ where $\alpha_1, \alpha_2 \in GF(2)$. Maximum value of HACR function for $\tau \neq 0$, is $1/3$ and maximum value of HCCR function is $1/3$.

4.4.3 Hamming Correlation Functions of Sequences Over Orthogonal Ideals of the Same Order in Semisimple $P_p^n[W(a)]$ Rings

We now give some results on HACR and HCCR functions of sequences over the orthogonal ideals in semisimple $P_p^n[W(a)]$. Consider a nonsingular canonical single output $P_p^n[W(a)]$ -LSS. Let $P_p^n[W(a)]$ be semisimple i.e., $W(a) = \prod_{i=1}^{\nu} W_i(a)$; $W_i(a)$ irreducible polynomial over $GF(p)$. Then $P_p^n[W(a)] = J_1 + J_2 + \dots + J_{\nu}$. If $n_i = \frac{n}{\nu}$ for all i , then the ideals J_i are of the same order p^{n_i} and $J_i \cong P_p^{n_i}[W_i(a)] \cong GF(p^{n_i})$, $i = 1, 2, \dots, \nu$. Further the common element in J_i and J_j for all i, j , $i \neq j$, is $0 \in P_p^n[W(a)]$. Suppose the characteristic polynomial $f(x)$ associated with the LRR is such that, $\tilde{f}_i(x) = f(x) \text{ modulo } [p; W_i(a)]$ is primitive over $P_p^{n_i}[W_i(a)]$; $i = 1, 2, \dots, \nu$, then for nonzero initial states with components from the ideal J_i , the period of any output sequence is $(p^{n_i K} - 1) \triangleq T$; which implies that the output sequence is isomorphic to maximum length sequence over $GF(p^{n_i})$. The number of zeros in such a sequence is $(p^{n_i(K-1)} - 1)$. Hence for $\tau \neq 0$, the maximum value of HACR function is $(p^{n_i(K-1)} - 1)$. Consider two sequences y over J_i and z over J_j , $i \neq j$. These sequences have equal period $T = (p^{n_i K} - 1)$ and have identical HACR function. Since there is no element in common in J_i and J_j other than $0 \in P_p^n[W(a)]$, the value of HCCR function is atmost $(p^{n_i(K-1)} - 1)$.

Example 4.4.11

Consider $P_2^2[a^2+a]$. $(a^2+a) = a.(a+1)$ is a product of two irreducible polynomials. Hence $P_2^2[a^2+a]$ is semisimple. Let $W_1(a) = a$ and $W_2(a) = (a+1)$.

It is easy to see that $e_1(a) = (a+1)$ and $e_2(a) = a$. Hence, $J_1 = \langle e_1(a) \rangle = \{0, (a+1)\}$ and $J_2 = \langle e_2(a) \rangle = \{0, a\}$. Consider a $P_2^2[a^2+a]$ -LRR with $f(x) = 1+x+x^3$.

We find the sequence s_1 with elements from J_1 and sequence s_2 with elements from J_2 . $f(x)$ modulo $[2, a]$ and $f(x)$ modulo $[2, a+1]$ are primitive. Hence these sequences will have maximum length i.e. $(2^3-1) = 7$, and number of zeros is 3.

$$s_1 = ((a+1), 0, 0, (a+1), (a+1), (a+1), 0)$$

$$s_2 = (a, 0, 0, a, a, a, 0)$$

and

$$H_{s_1}(\tau) = \begin{cases} 7 & ; & \tau = 0 \\ 3 & ; & \tau \neq 0 \end{cases} ; \quad H_{s_2}(\tau) = \begin{cases} 7 & ; & \tau = 0 \\ 3 & ; & \tau \neq 0 \end{cases}$$

i.e. the sequence of HACR and HCCR function values are

$$7, 3, 3, 3, 3, 3, 3,$$

$$7, 3, 3, 3, 3, 3, 3,$$

and $3, 1, 1, 1, 1, 1, 1$ respectively.

Example 4.4.12

Consider $P_2^6[(a^3+a+1)(a^3+a^2+1)]$; Let $A = \begin{bmatrix} 0 & 1 \\ a & a \end{bmatrix}$ and

$$f(x) = 1+ax+ax^2. \quad P_2^6[(a^3+a+1)(a^3+a^2+1)] \simeq P_2^3[a^3+a+1] \quad (4)$$

$$P_2^3[a^3+a^2+1],$$

$$\tilde{f}_1(x) = 1+ax+ax^2 \text{ modulo } [2; a^3+a+1]$$

$$= (1+ax+ax^2) \text{ which is primitive over } P_2^3[a^3+a+1]$$

$$\tilde{f}_2(a) = 1+ax+ax^2 \text{ modulo } [2; a^3+a^2+1]$$

$$= (1+ax+ax^2) \text{ which is primitive over } P_2^3[a^3+a^2+1].$$

We have, $W_1(a) = (a^3+a+1)$ and $\overline{W}_1(a) = (a^3+a^2+1)$, and

$W_2(a) = (a^3+a^2+1)$ and $\overline{W}_2(a) = (a^3+a+1)$. There exists

$$b_1(a) = a^3 \text{ and } b_2(a) = a \text{ such that } \overline{W}_1(a) \cdot b_1(a) + \overline{W}_2(a) \cdot b_2(a) \\ = 1 \text{ modulo } P_2^6[W(a)] .$$

Then, $\overline{W}_1(a) \cdot b_1(a) = e_1(a) = (a^4+a^2+a+1)$ and

$$\overline{W}_2(a) \cdot b_2(a) = e_2(a) = (a^4+a^2+a). \text{ Therefore,}$$

$$J_1 = \langle a^4+a^2+a+1 \rangle \text{ and } J_2 = \langle a^4+a^2+a \rangle .$$

s_1 has length 63. Let s_1^i be a part of sequence s_1 of length 9 we have

$$s_1^i = (a^4+a^2+a, 0, a^5+a^3+a^2, a^6+a^4+a^3, a^6+a^2+1, a^6+a^5+a, \\ a^5+a^3+a^2, a^5+a^4+1, a^5+a^3+a^2).$$

$$\text{Then } s_1 = (s_1^i, (a^5+a^3+a^2)s_1^i, (a^5+a^3+a^2)^2 s_1^i, \dots, (a^5+a^3+a^2)^6 s_1^i..)$$

There are totally 7 zeros, one in each section of length 9. Likewise $s_2 = (s_2^1, (a^5+a^3+a^2+a) s_2^1, \dots (a^5+a^3+a^2+a)^6 s_2^1, \dots)$.

There are totally 7 zeros one in each section of length 9.

The HACR function values of s_1 or s_2 are

$$\{63, 7, 7, 7, \dots 7\}$$

The HCCR function value between s_1 and s_2 is $H_{s_1 s_2}(\tau)$ is either 0 or 7 which is periodic with period 9. The sequence is $\{7000000007000000007000000007\dots 700000000\}$.

*

4.4.4 Hamming Correlation Properties and Hamming Weight-

Structure of Sequences Generated by Second Order LSS Over Semisimple $P_p^n[W(a)]$ Rings

In this subsection we consider a specific case of output sequences of second order, nonsingular, canonical, autonomous $P_p^n[W(a)]$ -LSS with $C = [1 \ 0]$. As before $P_p^n[W(a)]$ is semisimple i.e., $W(a) = W_1(a) \cdot W_2(a)$, where $W_i(a)$ is irreducible polynomial of degree n_i over $GF(p)$; $i = 1, 2, \dots$. The characteristic matrix A is such that, $\tilde{A}_i = A \text{ modulo } [p; W_i(a)]$ has period $= (p^{2n_i} - 1)$, $i = 1, 2$, or in terms of the characteristic polynomial $f(x)$ of the associated LRR $f(x)$ is such that $\tilde{f}_i(x) = f(x) \text{ mod } [p; W_i(a)]$ is primitive over $P_p^{n_i}[W_i(a)]$; $i = 1, 2, \dots$. It is then possible to obtain analytically, the number of levels and values of HACR and HCCR functions of sequences of length T . Here T is the period of matrix A and is equal to $\text{lcm} [(p^{2n_1} - 1), (p^{2n_2} - 1)]$. We make

use of the properties of maximum length sequences over finite fields given in [28].

We first prove the following lemmas.

Lemma 4.4.9

Let sequence S_T be set of solutions of second order $P_p^n[W(a)]$ -LRR, where $P_p^n[W(a)]$ is semisimple and the characteristic polynomial $f(x)$ of the LRR is as defined above. With initial values $([0 \ 1])$ over $P_p^n[W(a)]$, the sequence $s \in S_T$, has a period $T = \text{lcm} [(p^{2n_1}-1), (p^{2n_2}-1)]$ and the sequence $s_i = s.e_i(a)$ over J_i has a period $(p^{2n_i}-1)$; $i = 1, 2$.

Proof

From Lemma 4.3.6, period T of $f(x)$ is equal to $\text{lcm}[(p^{2n_1}-1), (p^{2n_2}-1)]$ and from Theorem 4.3.7, s over $P_p^n[W(a)]$ has a period T . $s.e_i(a) = s_i$ is a sequence over J_i and $J_i \simeq P_p^{n_i}[W_i(a)] \simeq \text{GF}(p^{n_i})$. $\tilde{f}_i(x)$ is primitive over $P_p^{n_i}[W_i(a)]$. Hence $s_i \simeq \tilde{s}_i$; $i = 1, 2$, where \tilde{s}_i is a maximum length sequence over $P_p^{n_i}[W_i(a)] \simeq \text{GF}(p^{n_i})$. Hence s_i has a period $(p^{2n_i}-1)$; $i = 1, 2$.

Lemma 4.4.10

In the sequence s_i of period $(p^{2n_i}-1)$ over J_i , the number of zeros is equal to $(p^{n_i}-1)$ and occur periodically with a

period

$$\theta_i = \frac{(p^{2n_i}-1)}{(p^{n_i}-1)} \quad i = 1, 2.$$

Proof

Consider a maximum length sequence \tilde{s}_i over $P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$; $i = 1, 2$. From the property (ii), given in Subsection 4.4.1, of maximum length sequence over finite fields, number of zeros in \tilde{s}_i is $(p^{n_i}-1)$. Further \tilde{s}_i has $(p^{n_i}-1)$ sections. From property (iv), if \tilde{s}_i is a part of the sequence of length $\frac{(p^{2n_i}-1)}{(p^{n_i}-1)} = \theta_i$, then the sequence \tilde{s}_i is $\tilde{s}_i = \{\tilde{s}_i^1, \alpha \tilde{s}_i^1, \dots, \alpha^{p^{n_i}-2} \tilde{s}_i^1\}$, where α is a primitive element in $P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i})$; $i = 1, 2$. Let j th element ${}_i y_j$ in \tilde{s}_i^1 be a zero then ${}_i y_j = 0$ and ${}_i y_{j+\theta_i} = \alpha {}_i y_j = 0$. In general,

$${}_i y_{j+m\theta_i} = \alpha^m {}_i y_j = 0; \quad m = 0, 1, 2, \dots \quad (4.4.7)$$

Since there are only $(p^{n_i}-1)$ zeros and these are equal number of sections in \tilde{s}_i , from Equation (4.4.7) it follows that each section has a single zero which occurs periodically with period θ_i , $i = 1, 2$, in $\tilde{s}_i \rightarrow s_i$ over J_i is isomorphic to \tilde{s}_i and hence the properties of \tilde{s}_i carry over to s_i .

The results of the Lemmas 4.4.9 and 4.4.10 are used in the computation of values of Hamming correlation functions of sequences in S_T . The length of sequences in S_T is $T = \text{lcm}[(p^{2n_1}-1), (p^{2n_2}-1)]$. s_1 and s_2 , are maximum length sequences over J_1 and J_2 respectively with only zero as the

common element in them. Any sequence in S_T can be expressed as s_1+s_2 , or its cyclic shifts. Consider sequence of the form $\sigma^T s_1+s_2$. An element at a given location in $(\sigma^T s_1+s_2)$ is a zero iff $\sigma^T s_1$ and s_2 have zeros at the same location. Hence the number of zeros in $(\sigma^T s_1+s_2)$ depends on the number of sections $(p^{n_1}-1)$ and $(p^{n_2}-1)$ and also the length of each

section $\theta_1 = \frac{(p^{2n_1}-1)}{(p^{n_1}-1)}$, $\theta_2 = \frac{(p^{2n_2}-1)}{(p^{n_2}-1)}$ in s_1 and s_2 respectively.

s_2 in S_T is of length T . Let there be j sections of length θ_2 . With one zero in each section, there are in all j zeros in the sequence s_2 of length T . s_1 in S_T is also of length T ; it has sections of length θ_1 . A zero in sequence s_2 can coincide with a zero in sequence $\sigma^T s_1$, in each part of the sequence of length which is an integral multiple of both θ_2 and θ_1 , i.e., $i_1\theta_1 = i_2\theta_2$; i_1, i_2 integers. Since θ_1 divides $i_1\theta_1$, θ_1 should divide $i_2\theta_2$. Hence the number of zeros in $\sigma^T s_1+s_2$ can be either nil or the number of integers in the set $\{\theta_2, 2\theta_2, 3\theta_2, \dots, j\theta_2\}$ that are divisible by θ_1 . This number is obtained in the following lemma.

Lemma 4.4.11

Let θ_1, θ_2, j be positive integers. Let $\theta_1 < \theta_2$. Then in the set of integers $\{\theta_2, 2\theta_2, 3\theta_2, \dots, (j-2)\theta_2, (j-1)\theta_2, j\theta_2\}$, the number of integers divisible by θ_1 is given by the greatest integer $\leq \frac{j}{\theta_1} \gcd(\theta_1, \theta_2)$.

Proof

We divide the proof into three parts where each part considers one of the possible cases : i) $\gcd(\theta_1, \theta_2) = \theta_1$;
 ii) $\gcd(\theta_1, \theta_2) = 1$; iii) $\gcd(\theta_1, \theta_2) > 1$.

(i) $\gcd(\theta_1, \theta_2) = \theta_1$. In this case $\theta_1 | \theta_2$ and hence all the j integers are divisible by θ_1 .

(ii) $\gcd(\theta_1, \theta_2) = 1$. In this case $\theta_1 \nmid \theta_2$ and hence θ_1 divides any integer $i\theta_2$ if it divides i . Hence number of integers in $\theta_2, 2\theta_2, \dots, j\theta_2$, that are divisible by θ_1 is the quotient of $\frac{j}{\theta_1}$, i.e., greatest integer $\leq \frac{j}{\theta_1} \gcd(\theta_1, \theta_2)$.

(iii) $\gcd(\theta_1, \theta_2) > 1$. Let $\gcd(\theta_1, \theta_2) = \beta$, where $1 < \beta < \theta_1$. By definition $\beta | \theta_1, \beta | \theta_2$. Let $\frac{\theta_1}{\beta} = \theta'_1, \frac{\theta_2}{\beta} = \theta'_2$. Then, $\gcd(\theta'_1, \theta'_2) = 1$.

If $\theta_1 | i\theta_2$, then $\theta'_1 | i\theta'_2$. Since $\gcd(\theta'_1, \theta'_2) = 1$, it follows that $\theta'_1 | i$. Thus the number of integer divisible by θ_1 is equal to the quotient of $\frac{j}{\theta'_1}$. This is equal to the greatest integer $\leq \frac{j}{\theta'_1} = \frac{j}{\theta_1} \gcd(\theta_1, \theta_2)$.

The result of Lemma 4.4.11 is used for the determination of the possible number of zeros in any sequence $s \in S_T$, which gives the possible values of Hamming correlation functions and the number of nonzero elements in a sequence in S_T which is the Hamming weight of the sequence. The set of Hamming weights w of sequences in S_T and the corresponding number of sequences of

weight w constitute the weight structure of sequences in S_T . The weight structure of sequences in S_T can be utilized to study the weight structure of error correcting codes over $P_p^n[W(a)]$ considered in Chapter 5.

In what follows we consider examples of sequences of length T which are solutions of second order $P_p^n[W(a)]$ -LRR, where $P_p^n[W(a)]$ is semisimple and isomorphic to external direct sum of two finite fields. Further the characteristic polynomial $f(x)$ of LRR is such that $\tilde{f}_i(x) = f(x) \text{ modulo } [p; W_i(x)]$ is primitive. In these examples the possible values of Hamming correlation functions and the weight structure of the sequences are found.

Example 4.4.13

Consider semisimple $P_2^3[a^3+1]$. $(a^3+1) = (a+1)(a^2+a+1)$.

$n_1 = 1, n_2 = 2, e_1(a) = (a^2+a+1), e_2(a) = (a^2+a);$

$J_1 = \langle e_1(a) \rangle \simeq GF(2)$ and $J_2 = \langle e_2(a) \rangle \simeq GF(2^2)$.

Since $\tilde{f}_i(x)$ is of degree 2 and is primitive over $P_2^{n_i}[W_i(a)]$;

$$i = 1, 2,$$

s_1 over J_1 , is of period $(2^2-1) = 3, \theta_1 = 3$ and number of zeros 1, s_2 over J_2 is of period $(2^2)^2-1 = 15, \theta_2 = 5$ and number of zeros = 3. $j = \frac{15}{\theta_2} = 3$. Consider s_1 and s_2 of length 15.

Number of zeros in $\sigma^{\tau} s_1 + s_2$ is either zero or greatest integer

$$\leq \frac{j}{\theta_1} \gcd(\theta_2, \theta_1) \leq \frac{3}{3} \gcd(5, 3) = 1.$$

The weight structure is given in Table 4.4.1.

Table 4.4.1 Weight Structure of Sequences of Example 4.4.13

Weight of sequence	Number of sequences
0	1
10	3
12	15
14	45

Example 4.4.14

Consider semisimple $P_2^4[(a+1)(a^3+a+1)] = J_1 + J_2$.

$n_1 = 1, n_2 = 3$; $J_1 \simeq P_2^1[a+1] \simeq GF(2)$; $J_2 \simeq P_2^3[a^3+a+1] \simeq GF(2^3)$.

Since $\tilde{f}_1(x)$ is of degree 2 and is primitive over $P_2^{n_i}[W_i(a)]$,

$$i = 1, 2.$$

s_1 over J_1 is of period $(2^2-1) = 3$, s_2 over J_2 is of period $(2^3)^2-1 = 63$. $T = 63$. Number of zeros in s_1 is 21, $\Theta_1 = 3$.

Number j of sections in s_2 is $(2^3-1) = 7$ and number of zeros in s_2 is 7. Thus $\Theta_2 = \frac{63}{7} = 9$. Number of zeros in $\sigma^\tau s_1 + s_2$ is either zero or greatest integer $\leq \frac{j}{\Theta_1} \gcd(\Theta_2, \Theta_1) = \frac{7}{3} \gcd(3, 63) = 7$. Period of s_1 is 3 and $\Theta_2 = 9$. Hence whenever a zero of $\sigma^\tau s_1$ coincides with a zero of s_2 all the other zeros of s_2 also

However, for each τ , a zero of σs_1 coincides with a zero of s_2 . Hence number of zeros in $s_1 + s_2$ is one. The number of possible zeros in sequences (of length 15) in S_T are computed as follows. Any sequence in S_T is of the form $\sigma^\tau + \sigma^{\tau_2} s_2$. Number of zeros in s_1 or its cyclic shifts is 5. Number of zeros in s_2 or its cyclic shifts is 3. Number of zeros in other sequences is 1. Corresponding normalised values are $\frac{1}{3}, \frac{1}{5}, \frac{1}{15}$. Thus possible normalised values of HACR functions of sequence in S_T is $\{1, \frac{1}{3}, \frac{1}{5}, \frac{1}{15}\}$. Possible normalised values of HCCR function between two sequences is $\{\frac{1}{3}, \frac{1}{5}, \frac{1}{15}\}$.

The Hamming weight structure of 64 sequences in S_T is computed as follows:

The sequences in S_T can be s_1 or s_2 or their cyclic shifts, or sum of $\sigma^{\tau_1} s_1$ and $\sigma^{\tau_2} s_2$ over $p_2^3[a^3+1]$, where

$\tau_1 < 3$ and $\tau_2 < 15$, are nonnegative integers. The weight of s_1 or its cyclic shifts is 10. Since s_1 is of period 3 there are 3 sequences of weight 10. The weight of s_2 or its cyclic shifts is 12. Since s_2 is of period 15 there are 15 sequences of weight 12. When the sequence is a sum of $\sigma^{\tau_1} s_1$ and $\sigma^{\tau_2} s_2$, since s_1 is of period 3 and s_2 is of period 15, there results 45 sequences. Further in each of these sequences since only one zero of $\sigma^{\tau_1} s_1$ coincides with a zero of $\sigma^{\tau_2} s_2$, these 45 sequences are of weight 14. The zero sequence is of weight zero.

coincide with zero of $\sigma^{\tau_1} s_1$. Otherwise the number of zeros in $\sigma^{\tau_1} s_1$ is zero. Thus, number of zeros in s_1 or its cyclic shifts is 21, number of zeros in s_2 or its cyclic shifts is 7, and number of zeros in $\sigma^{\tau_1} s_1 + \sigma^{\tau_2} s_2$ is either zero or 7.

Possible values of HACR function are $\{63, 21, 7, 0\}$

Possible normalised values of HACR function are $\{1, \frac{1}{3}, \frac{1}{9}, 0\}$.

Possible normalised values of HCCR function between sequences in S_T is $\{\frac{1}{3}, \frac{1}{9}, 0\}$.

The Hamming weight structure of 256 sequences in S_T is computed as follows. The sequences in S_T can be s_1 , or s_2 or their cyclic shifts of sum of $\sigma^{\tau_1} s_1 + \sigma^{\tau_2} s_2$ over $P_2^4[(a+1)(a^3+a+1)]$, where $\tau_1 < 3$ and $\tau_2 < 63$, are nonnegative integers. The weight of s_1 or its cyclic shifts is 42. Since s_1 is of period 3 there are 3 sequences of weight 42. The weight of s_2 or its cyclic shift is 59. Since s_2 is of period 63 there are 63 such sequences of weight 59. Further for a given value of τ_1 , a zero of $\sigma^{\tau_1} s_1$ coincides with $\sigma^{\tau_2} s_2$ for 7 values of τ_2 . Since τ_1 takes three values namely 0, 1, 2, there are totally 21 such sequences of weight 59. Hence there are $(63+21) = 84$ sequences of weight 59. The remaining sequences will have weight 63. The weight structure is given in Table 4.4.2.

Table 4.4.2 Weight Structure of Sequences of Example 4.4.14

Weight of sequence	Number of sequences
0	1
42	3
59	84
63	168

4.5 SET OF ORTHOGONAL SEQUENCES OVER ORTHOGONAL IDEALS IN $P_p^n[W(a)]$

As we have seen in Section 2.4, an element $r(a)$ in a semi-local or a semisimple $P_p^n[W(a)]$ can be decomposed into internal direct sum components where each component is from an orthogonal ideal. These components mutually annihilate each other. Thus sequences over distinct orthogonal ideals are inherently elementwise orthogonal. In this section we give techniques for (i) generation of set of sequences over orthogonal ideals in $P_p^n[W(a)]$ (ii) decomposition of sequences over $P_p^n[W(a)]$ into set of orthogonal sequences over the same ring and (iii) transformation of sequences over primary ring or direct sum of primary rings into set of orthogonal sequences over appropriate larger rings. It is shown that arbitrary sequences over semi-local or semisimple ring can be decomposed into sets of orthogonal sequences over a larger semilocal or semisimple rings which

contains orthogonal ideals isomorphic to the orthogonal ideals in the smaller rings. Examples are included to illustrate the techniques for generation of sets of orthogonal sequences, decomposition and transformation of sequences into set of orthogonal sequences. Application of orthogonal sequences for multiplexing and modulation is taken up in the next section.

Consider two sequences of equal length N

$$V^{(1)} = (V_0^{(1)}, V_1^{(1)}, V_2^{(1)}, \dots, V_{N-1}^{(1)}) \quad (4.5.1)$$

and

$$V^{(2)} = (V_0^{(2)}, V_1^{(2)}, V_2^{(2)}, \dots, V_{N-1}^{(2)}) \quad (4.5.2)$$

of equal length N over arbitrary field. We call, $V^{(1)} \cdot V^{(2)} = \sum_{i=0}^{N-1} V_i^{(1)} \cdot V_i^{(2)}$, the inner product of the two sequences $V^{(1)}$ and

$V^{(2)}$. Sequences $V^{(1)}$ and $V^{(2)}$ are said to be orthogonal if their inner product is zero. In what follows we see that, if the sequences are over distinct orthogonal ideals, each of the elementwise products is identically equal to zero.

Let $P_p^n[W(a)]$ be a semilocal ring, where $W(a) = \prod_{i=1}^{\nu} W_i^{h_i}(a)$.

$W_i(a)$ irreducible polynomial of degree n_i over $GF(p)$. We have seen in Section 2.4 that the ring $P_p^n[W(a)]$ contains ν orthogonal idempotents $e_i(a)$; $i = 1, 2, \dots, \nu$. Each orthogonal idempotent $e_i(a)$ generates an orthogonal ideal J_i and $P_p^n[W(a)]$ is the internal direct sum of J_i ; $i = 1, 2, \dots, \nu$. Any element

$r(a) \in P_p^n[W(a)]$ is uniquely given by the internal direct sum
 $r(a) = r_1(a) + r_2(a) + \dots + r_i(a) + \dots + r_\nu(a)$ modulo $[p; W(a)]$,
 where $r_i(a)$ is a multiple of $e_i(a)$ and hence belongs to J_i ,
 $i = 1, 2, \dots, \nu$. If $r(a)$ is $0 \in P_p^n[W(a)]$ all the components
 are zeros. If $r(a)$ is a zero divisor in $P_p^n[W(a)]$ at least one
 component is zero. The internal direct sum components $r_i(a)$;
 $i = 1, 2, \dots, \nu$ of $r(a)$ has orthogonal property as proved in
 the following lemma.

Lemma 4.5.1

Let $r(a) = r_1(a) + r_2(a) + \dots + r_i(a) + \dots + r_\nu(a)$
 modulo $[p; W(a)]$, where $r_i(a) \in J_i$; $i = 1, 2, \dots, \nu$. Then,
 $r_i(a) = r(a) \cdot e_i(a)$ modulo $[p; W(a)]$; $i = 1, 2, \dots, \nu$ and
 $r_i(a) \cdot r_j(a) = 0$ modulo $[p; W(a)]$; $i = 1, 2, \dots, \nu$; $i \neq j$.

Proof

$r(a) = r_1(a) + r_2(a) + \dots + r_i(a) + \dots + r_\nu(a)$
 modulo $[p; W(a)]$. $r(a) \cdot e_i(a) = r_1(a) \cdot e_i(a) + r_2(a) \cdot e_i(a) + \dots +$
 $r_i(a) \cdot e_i(a) + \dots + r_\nu(a) \cdot e_i(a)$ modulo $[p; W(a)]$.

$r_j(a) \in J_j$ and hence is a multiple of $e_j(a)$; $j = 1, 2, \dots, \nu$.

From the property of orthogonal idempotents

$$e_i(a) \cdot e_j(a) = 0 \text{ modulo } [p; W(a)] ; \quad \begin{matrix} i, j = 1, 2, \dots, \nu \\ j \neq i \end{matrix}$$

and $r_i(a) \cdot e_i(a) = r_i(a)$ modulo $[p; W(a)]$.

Thus $r_i(a) = r(a) \cdot e_i(a)$ modulo $[p; W(a)]$. $r_i(a)$ is a multiple of $e_i(a)$ and $r_j(a)$ is a multiple of $e_j(a)$.

Hence $r_i(a) \cdot r_j(a) = 0$ modulo $[p; W(a)]$, $i, j = 1, 2, \dots, \nu; i \neq j$.

If z is a sequence over $P_p^n[W(a)]$, the sequence can be viewed as a direct sum of ν sequences $z^{(i)}$; where elements of $z^{(i)}$ are from the orthogonal ideals J_i ; $i = 1, 2, \dots, \nu$. Consider sequences,

$$z^{(1)} = (z_0^{(1)}, z_1^{(1)}, \dots, z_{N-1}^{(1)}) \quad (4.5.3)$$

$$z^{(2)} = (z_0^{(2)}, z_1^{(2)}, \dots, z_{N-1}^{(2)}) \quad (4.5.4)$$

of equal length N which are over two distinct orthogonal ideals in $P_p^n[W(a)]$. From the above lemma it is seen that, the elements of $z^{(1)}$ and $z^{(2)}$ mutually annihilate, that is $z_j^{(1)} \cdot z_j^{(2)} = 0$ modulo $[p; W(a)]$; for all $j = 0, \dots, N-1$. Hence $z^{(1)}$ and $z^{(2)}$ are said to be orthogonal to each other. However, the orthogonality is not in the usual inner product sense. In general, if $P_p^n[W(a)]$ is equal to the internal direct sum of ν orthogonal ideals, J_i ; $i = 1, \dots, \nu$, the sequences $z^{(1)}, z^{(2)}, \dots, z^{(\nu)}$ over J_1, J_2, \dots, J_ν respectively, constitute a set of orthogonal sequences.

In what follows we study different techniques for obtaining sets of orthogonal sequences over semilocal or over semisimple ring. A motivation for this study is the application of these orthogonal sequences in modulation and multiplexing of data

sequences, which we will discuss in Section 4.6.

The techniques are broadly classified into three types, based on the following :

- 1) Generation of sets of orthogonal sequence which are autonomous responses of canonical and single output LSS over semilocal or semisimple ring, $P_p^n[W(a)]$, with specified initial conditions.
- 2) Decomposition of a sequence over semilocal or semisimple ring $P_p^n[W(a)]$ into orthogonal sequences over orthogonal ideals in $P_p^n[W(a)]$.
- 3) Transformation of sequences over primary ring or direct sum of primary rings, $P_p^n[W(a)]$ into orthogonal sequences over larger semisimple or semilocal rings which contains orthogonal ideals isomorphic to $P_p^n[W(a)]$.

4.5.1 Generation of Orthogonal Sequences

Consider a Kth order singular canonical single output $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$. Let $P_p^n[W(a)]$ be a semilocal ring. We have seen in Section 4.3 that when the elements a_i ; $i = 1, 2, \dots, K$ in the characteristic matrix A_c are from an orthogonal ideal J_j and further if a_K is not a nilpotent element in J_j , the output sequences with initial state having components from J_j , are periodic. These sequences have elements from J_j . If $P_p^n[W(a)]$ is an internal direct sum of ν orthogonal ideals, orthogonal sequences can be generated from ν generators.

We have $J_j \simeq P_p^{h_j n_j} [W_j^{h_j}(a)]$.

If $h_j = 1$, then J_j is isomorphic to $GF(p^{n_j})$. Then for $a_i \neq 0$; $i = 1, 2, \dots, K$ and initial values from J_j , the sequences are periodic and are isomorphic to sequences over $P_p^{n_j} [W_j(a)] \simeq GF(p^{n_j})$. Further for proper choice of $a_1, a_2, \dots, a_K \in J_j$, the periodic output sequence is isomorphic to a maximum length sequence of period $(p^{n_j K} - 1)$ over $GF(p^{n_j})$.

If $h_1 = h_2 = \dots, h_\nu = 1$, the ring $P_p^n [W(a)]$ is semisimple. Each orthogonal ideal is isomorphic to a finite field of the same order. The orthogonal sequence over J_i is then isomorphic to sequence over $GF(p^{n_i})$; $i = 1, 2, \dots, \nu$.

Orthogonal sequence over $P_p^n [W(a)]$ can also be generated using a nonsingular canonical single output $P_p^n [W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$. However, in this case for generating sequence $Z^{(i)}$ over J_i , the initial state must have components from J_j .

The sequences over $P_p^n [W(a)]$ can also be viewed as sequences of n -tuples over $Z_p^n [W] \simeq P_p^n [W(a)]$.

The generation of sets of orthogonal sequences over semi-local and semisimple rings is taken up in the following examples.

Example 4.5.1

Consider the semisimple ring $P_2^3 [a^3+1]$. $(a^3+1) = (a+1)(a^2+a+1)$. The orthogonal idempotents are $e_1(a) = (a^2+a+1)$

and $e_2(a) = (a^2 + a)$. The orthogonal ideals are, $J_1 = \langle e_1(a) \rangle = \{0, 1 + a + a^2\} \simeq \text{GF}(2)$ and $J_2 = \langle e_2(a) \rangle = \{0, (a + a^2), (1 + a^2), (1 + a)\} \simeq \text{GF}(2^2)$. Consider singular, autonomous second order single output system over J_1 with characteristic matrix

$$A_c = \begin{bmatrix} 0 & 1 \\ 1 + a + a^2 & 1 + a + a^2 \end{bmatrix} \quad \text{and } C = [1 \ 0]. \quad |A_c| = 1 + a + a^2$$

is a zero divisor in $P_2^3[a^3 + 1]$ and A_c is not nilpotent. Hence, the system is singular. With the initial state $[0, 1 + a + a^2]^{\text{tr}}$, the output sequence is $z^{(1)} = (0, 1 + a + a^2, 1 + a + a^2, 0, \dots)$. The sequence is periodic with period $(2^2 - 1) = 3$ and is isomorphic to a maximum length sequence over $\text{GF}(2)$. The number of sequences is equal to the number of distinct nonzero initial states, that is 3

Likewise a singular autonomous second order single output

system over J_2 with $A_c = \begin{bmatrix} 0 & 1 \\ 1 + a & a + a^2 \end{bmatrix}$ and $C = [1 \ 0]$, gene-

rates orthogonal sequence $z^{(2)}$ over J_2 . Here $|A_c| = (1 + a)$ which is a zero ^{divisor} in $P_2^3[a^3 + 1]$. Hence the system is singular (A_c is not nilpotent). With the initial state $[0, 1 + a]^{\text{tr}}$, the output sequence is

$$z^{(2)} = (0, 1 + a, 1 + a, a + a^2, 1 + a, 0, 1 + a^2, 1 + a^2, 1 + a, 1 + a^2, 0, a + a^2, a + a^2, 1 + a^2, a + a^2, 0, \dots)$$

The sequence is periodic with period $(2^2)^2 - 1 = 15$, and is

isomorphic to a maximum length sequence over $GF(2^2)$. The number of sequences is equal to the number of distinct nonzero initial states, i.e., 15. We note that segments of same length of sequences $Z^{(1)}$ and $Z^{(2)}$ are orthogonal, as the individual sequence elements are orthogonal.

The normalised HACR function of sequences $Z^{(1)}$ and $Z^{(2)}$ and (ii) the HCCR function between $Z^{(1)}$ and $Z^{(2)}$ are given below. $H_{Z^{(1)}}(\tau) = (1, \frac{1}{3}, \frac{1}{3})$; $H_{Z^{(2)}}(\tau) = (1, \frac{1}{5}, \frac{1}{5}, \dots)$ and $H_{Z^{(1)}Z^{(2)}}(\tau)$ is of length 15 and has two levels 0 and $\frac{1}{5}$.

In this example the sequences can also be viewed as sequences over $Z_2^3 \cong P_2^3[a^3+1]$. The implementation of sequences generators is obtained as discussed in Section 3.5. The sequence $Z^{(1)}$ and $Z^{(2)}$ of 3-tuples over $GF(2)$, isomorphic to $Z^{(1)}$ and $Z^{(2)}$ respectively is given below.

$$\underline{Z}^{(1)} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 & \dots \\ 0 & 1 & 1 \end{pmatrix} \cong Z^{(1)}$$

$$\underline{Z}^{(2)} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & \dots \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \cong Z^{(2)}.$$

Example 4.5.2

Consider the semilocal ring $P_2^6[a^6+1]$. $(a^6+1) = (a+1)^2 (a^2+a+1)^2$. The orthogonal idempotents are :

$e_1(a) = (a^4 + a^2 + 1)$ and $e_2(a) = (a^4 + a^2)$. The orthogonal ideals are $J_1 = \langle e_1(a) \rangle = \{0, (1+a^2+a^4), (a+a^3+a^5), (1+a+a^2+a^3+a^4+a^5)\}$ $J_2 = \langle e_2(a) \rangle = \{0, (a^2+a^4), (a^3+a^5), (1+a^4), (a+a^5), (1+a^2), (a+a^3), (a^2+a^3+a^4+a^5), (a+a^2+a^4+a^5), (a+a^2+a^3+a^4), (1+a^3+a^4+a^5), (1+a^2+a^3+a^5), (1+a+a^4+a^5), (1+a+a^3+a^4), (1+a+a^2+a^5), (1+a+a^2+a^3)\}$. Consider the second order autonomous canonical single output system over J_1 given in Figure 4.5.1a. With the initial state $[(1+a^2+a^4), 0]^{\text{tr}}$ the sequence $Z^{(1)}$ generated is of period 6.

$$Z^{(1)} = \{(1+a^2+a^4), 0, (a+a^3+a^5), (a+a^3+a^5), (1+a+a^2+a^3+a^4+a^5), (a+a^3+a^5), (1+a^2+a^4), 0 \dots\}.$$

There are 15 nonzero initial states, which gives rise to 15 sequences. Consider the second order autonomous canonical single output system over J_2 given in Figure 4.5.1b. With the initial state $[(a^3+a^5), 0]^{\text{tr}}$ the sequence generated is of period 3.

$Z^{(2)} = \{(a^3+a^5), 0, a^3+a^5, \dots\}$. There are 255 nonzero initial states and hence 255 sequences. The sequences $Z^{(1)}$ and $Z^{(2)}$ are orthogonal. The common element in sequences $Z^{(1)}$ and $Z^{(2)}$ is the zero of the ring. Considering a length $\text{lcm}(6, 3) = 6$ of the sequences $Z^{(1)}$ and $Z^{(2)}$, normalised cross-correlation $H_{Z^{(1)}Z^{(2)}}(\tau)$ is of two level 0 and $\frac{1}{6}$. The sequences can also be viewed as sequences over $Z_2^6 \cong P_2^6[a^6+1]$. The implementation of sequence generators is obtained as discussed in Section 3.5.

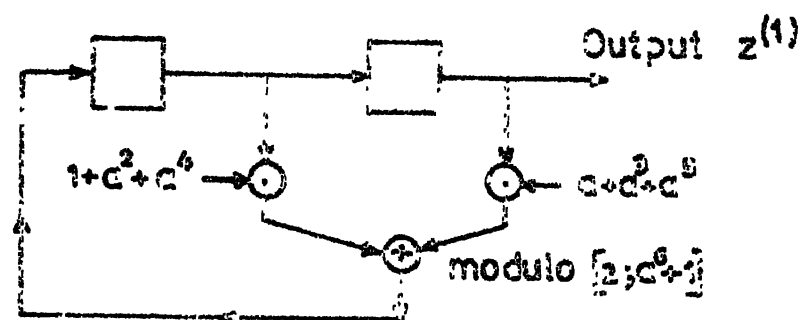


Fig. 4.5.1a Generation of Sequence $z^{(1)}$ of Example 4.5.1

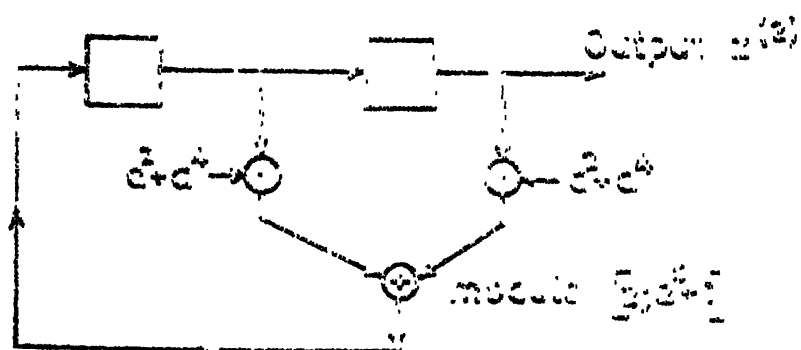


Fig. 4.5.1b Generation of Sequence $z^{(2)}$ of Example 4.5.1

The sequence $\underline{Z}^{(1)}$ of 6-tuples over GF(2) isomorphic to $Z^{(1)}$ is,

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

The sequence $\underline{Z}^{(2)}$ of 6-tuples over GF(2) isomorphic to $Z^{(2)}$ is,

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

4.5.2 Decomposition of Sequences

Consider a semilocal ring $P_p^n[W(a)]$. $W(a) = \sum_{i=1}^{\nu} W_i^{h_i}(a)$. As discussed earlier, any element $r(a) \in P_p^n[W(a)]$ can be uniquely expressed as the internal direct sum of ν components $r_i(a)$; where $r_i(a) \in$ the orthogonal ideal J_i ; $i = 1, 2, \dots, \nu$. Further from Lemma 4.5.1 we see that the component $r_i(a) = r(a) \cdot e_i(a) \text{ modulo } [p; W(a)]$, where $e_i(a)$ is orthogonal idempotent in $P_p^n[W(a)]$ and $r_i(a) \cdot r_j(a) = 0 \text{ modulo } [p; W(a)]; i \neq j$.

Let Z be any sequence over $P_p^n[W(a)]$. By multiplying each element of Z by $e_1(a)$ modulo $[p; W(a)]$ we get a sequence $Z^{(1)}$ over J_1 . Likewise $e_i(a) \cdot Z$ gives a sequence $Z^{(i)}$ over J_i $i = 1, 2, \dots, \nu$. Since the product of any element $r_i(a)$ of sequence $Z^{(i)}$ and any element $r_j(a)$ of sequence $Z^{(j)}$, $j \neq i$ gives zero modulo $[p; W(a)]$, the sequences, $Z^{(1)}, Z^{(2)}, \dots, Z^{(\nu)}$ are mutually orthogonal.

Thus the sequence Z over $P_p^n[W(a)]$ can be decomposed into orthogonal sequences. The scheme is given in Figure 4.5.2. We note here that the elements of sequence Z or $Z^{(i)}$; $i = 1, 2, \dots, \nu$ are polynomials of degree less than n and are elements of $P_p^n[W(a)]$. Z or $Z^{(i)}$, $i = 1, 2, \dots, \nu$, alternatively can be viewed as a sequence of n -tuples which are elements of $Z_p^n[W] \simeq P_p^n[W(a)]$. However, the elements of $Z^{(i)}$ are from an ideal in $Z_p^n[W]$ which is isomorphic to J_i ; $i = 1, 2, \dots, \nu$.

As we have seen in Section 2.4,

$$P_p^n[W(a)] \simeq P_p^{h_1 n_1}[W_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_\nu n_\nu}[W_\nu^{h_\nu}(a)]$$

and

$$P_p^n[W(a)] = J_1 + J_2 + \dots + J_\nu,$$

$$\text{and } J_i \simeq P_p^{h_i n_i}[W_i^{h_i}(a)].$$

$$\text{If } h_j = 1 \text{ then } J_j \simeq P_p^{n_j}[W_j(a)] \simeq GF(p^{n_j})$$

If $h_1 = h_2 = \dots = h_\nu = 1$, then the ring is semisimple and the orthogonal sequence over J_i , is isomorphic to sequence over $GF(p^{n_i})$; $i = 1, 2, \dots, \nu$.

Thus when the ring $P_p^n[W(a)]$ is a direct sum of primary rings a sequence Z over $P_p^n[W(a)]$ can be decomposed into orthogonal sequences over orthogonal ideals in $P_p^n[W(a)]$.

In the first method of generation of sequences discussed in Subsection 4.5.1, the number of generators required is equal to the number of orthogonal sequences. In the case of decomposition of sequence, a sequence Z from a single generator is decomposed into orthogonal sequences over the orthogonal ideals, using scalars, $e_i(a)$, $i = 1, 2, \dots, \nu$.

Example 4.5.3

Consider a second order autonomous canonical single output $P_2^3[a^3+1]$ -LSS, L as given in Figure 4.5.3a. The output sequence Z with the initial state $[1 \ 0]^{tr}$ is a periodic sequence of period 15.

$$Z = (1, 0, a, a^2, 1+a^2, a, 1+a+a^2, 1+a, 1, a^2, 1+a, 1+a+a^2, 1, 1+a^2, 1, 1, 0, \dots)$$

The sequence Z is decomposed into orthogonal sequences $Z^{(1)}$ over J_1 and $Z^{(2)}$ over J_2 , where $J_1 = \langle a^2+a+1 \rangle = \{0, 1+a+a^2\} \simeq P_2^1[a+1]$

and $J_2 = \langle a^2+a \rangle = \{0, (a+a^2), (1+a), (1+a^2)\} \simeq P_2^2[a^2+a+1]$.

The scheme of decomposition of Z into orthogonal sequences $Z^{(1)}$ and $Z^{(2)}$ over J_1 and J_2 respectively is given in Figure 4.5.3b.

$Z_{||}^{(1)} = \{(1+a+a^2), 0, (1+a+a^2), (1+a+a^2), 0, (1+a+a^2), (1+a+a^2), 0, \dots\}$ is a periodic sequence of period 3 over J_1 and

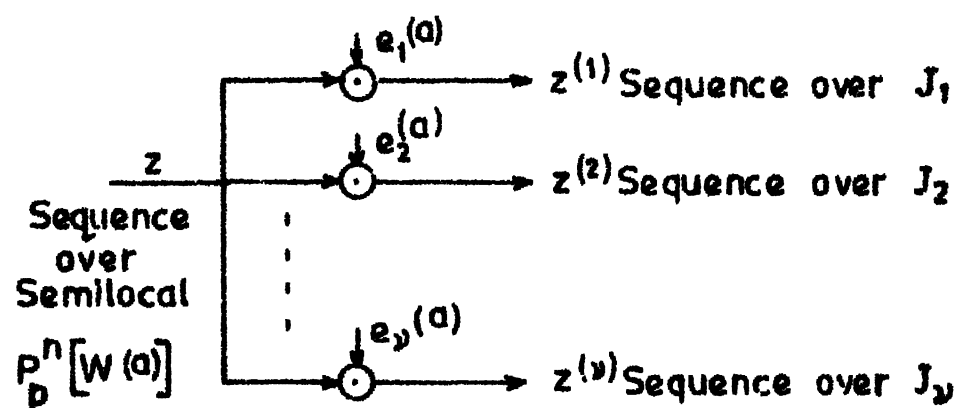


Fig.4.5.2 Decomposition of Sequence z over Semilocal $P_p^n[W(a)]$

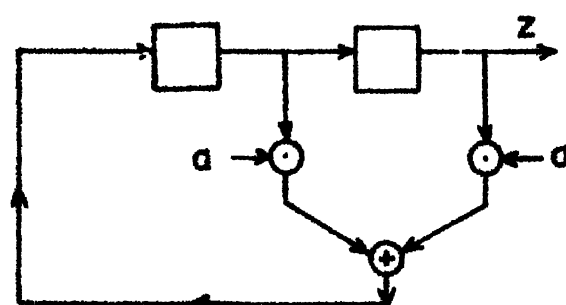


Fig.4.5.3a Generation of Sequence z of Example 4.5.3

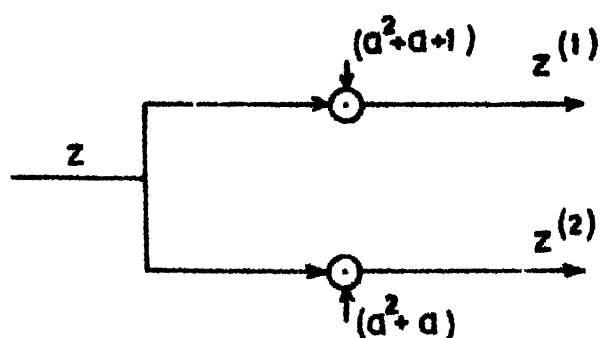


Fig.4.5.3b Decomposition of Sequence z of Example 4.5.3

$z^{(2)} = \{(a+a^2), 0, (1+a^2), (1+a), (1+a^2), (1+a^2), 0, (1+a), (a+a^2), (1+a), (1+a), 0, (a+a^2), (1+a^2), (a+a^2), (a+a^2), 0, \dots\}$ is a periodic sequence of period 15 over J_2 .

A Z_2^3 -LSS $L' \simeq L$ generates a sequence \underline{z} over Z_2^3 . This is decomposed into two orthogonal sequences $\underline{z}^{(1)}$ and $\underline{z}^{(2)}$ over Z_2^3 . Implementation of the sequence generator $L' \simeq L$ and the scalars are done as per the procedure outlined in Chapter 3.

The sequences over Z_2^3 are given below.

$$\underline{z} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \dots \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

and

$$\underline{z}^{(1)} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \dots \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

$$\underline{z}^{(2)} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \dots \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

4.5.3 Transformation of Sequence Over Local Rings into Orthogonal Sequences

Let $P_p^n[W(a)]$ be a semilocal ring; $W(a) = \prod_{i=1}^v W_i^{h_i}(a)$, then the local ring $P_p^{h_i n_i}[W_i^{h_i}(a)]$ is isomorphic to the orthogonal ideal J_i . We have seen in Section 2.4 that local ring $P_p^{h_i n_i}[W_i^{h_i}(a)]$ can be embedded in a semilocal ring $P_p^n[W(a)]$ by an appropriate isomorphic mapping. If $W_1(a), W_2(a), \dots, W_m(a)$ are irreducible polynomials of the same degree say n_1 and $h_1 = h_2 = \dots = h_m$, then the rings $P_p^{h_1 n_1}[W_1^{h_1}(a)], \dots, P_p^{h_m n_m}[W_m^{h_m}(a)]$ are isomorphic to each other and are isomorphic to the orthogonal ideals J_1, J_2, \dots, J_m in $P_p^n[W(a)]$. Let

$$\phi_{ij} : P_p^{h_1 n_1}[W_1^{h_1}(a)] \rightarrow J_j$$

be the isomorphic mapping between the local ring $P_p^{h_1 n_1}[W_1^{h_1}(a)]$ and the orthogonal ideal J_j . The corresponding inverse mapping is

$$\phi_{ij}^{-1} : J_j \rightarrow P_p^{h_1 n_1}[W_1^{h_1}(a)]$$

Consider a mapping or transformation ϕ_{ij} which maps elements from $P_p^{h_1 n_1}[W_1^{h_1}(a)]$ into elements of J_j with the rule

$$\begin{aligned} \phi_{ij} : \tilde{r}_i(a) \in P_p^{h_1 n_1}[W_1^{h_1}(a)] &\rightarrow \tilde{r}_i(a) \cdot e_j(a) \text{ modulo } [p; W(a)] \\ &= r_{ij}(a) \in J_j \end{aligned} \quad (4.5.5)$$

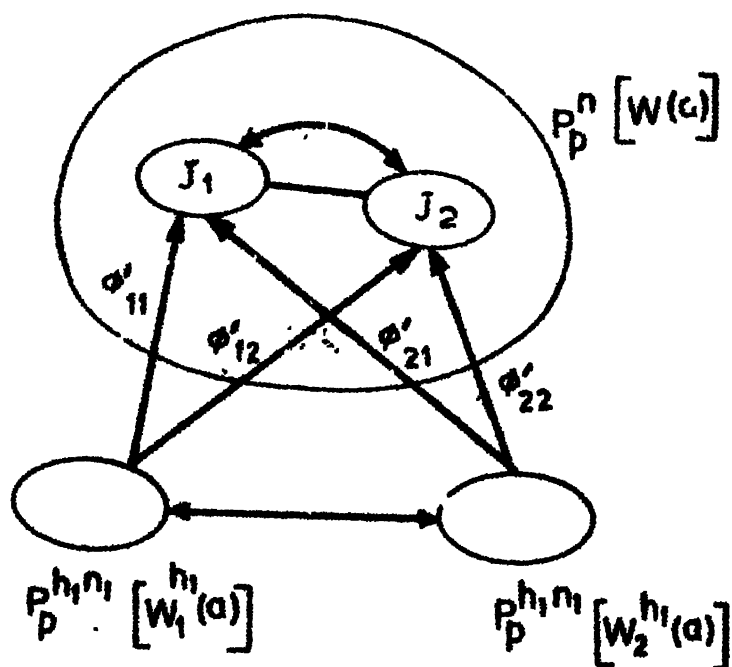
The corresponding inverse mapping is

$$\begin{aligned}\phi_{ij}^{-1} : r_{ij}(a) \in J_j &\rightarrow r_{ij}(a) \text{ modulo } [p; W_i^{h_1}(a)] \\ &= \tilde{r}_i(a) \in P_p^{h_1 n_1}[W_i^{h_1}(a)]\end{aligned}\quad (4.5.6)$$

For $i = j$, $\phi_{ij} = \phi'_{ij}$ is the isomorphism between the local ring $P_p^{h_1 n_1}[W_i^{h_1}(a)]$ and orthogonal ideal J_j . However, for $i \neq j$, ϕ_{ij} is an isomorphism only, between additive abelian group structures of $P_p^{h_1 n_1}[W_i^{h_1}(a)]$ and J_j .

The isomorphisms ϕ_{ij} are illustrated in Figure 4.5.4 for the case $m = 2$. The isomorphisms between J_1 and J_2 and $P_p^{h_1 n_1}[W_1^{h_1}(a)]$ and $P_p^{h_1 n_1}[W_2^{h_1}(a)]$ are also indicated.

The key notion in this technique is that an element in any of the m local rings is uniquely mapped into an element in each of the m orthogonal ideals by the isomorphisms. Thus if we have an arbitrary sequence over local ring $P_p^{h_1 n_1}[W_1^{h_1}(a)]$, the embedding of elements of this sequence in the orthogonal ideals J_1, J_2, \dots, J_m isomorphic to $P_p^{h_1 n_1}[W_1^{h_1}(a)]$ results in a set of m orthogonal sequences. In effect an arbitrary sequence over $P_p^{h_1 n_1}[W_1^{h_1}(a)]$ is transformed into a set of m orthogonal sequences over $P_p^n[W(a)]$. It is imperative in this scheme that $P_p^n[W(a)]$ should have at least one orthogonal ideal isomorphic to the local ring. If a sequence over a local ring $P_p^{h_1 n_1}[W_1^{h_1}(a)]$ is to be



$W_1(a), W_2(a)$ are irreducible polynomials of the same degree n_1 over $GF(p)$

Fig.4.5.4 Isomorphism Between Local rings and Orthogonal Ideals .

transformed into m orthogonal sequences, there must be a semilocal ring such that the local ring can be embedded into m orthogonal ideals isomorphic to each other. The number m of orthogonal signals is governed by the number of irreducible polynomials of degree n_1 over $GF(p)$ and the semilocal ring of least order is the direct sum of m local rings, $P_p^{h_j n_j}[W_j^{h_j}(a)]$; $j = 1, 2, \dots, m$.

$$\text{When } W(a) = \sum_{i=1}^v W_i(a)$$

$P_p^n[W(a)]$ is a semisimple ring

$$\text{and } P_p^{n_i}[W_i(a)] \simeq GF(p^{n_i}) \simeq J_i \quad i = 1, 2, \dots, v$$

The mapping of elements from $P_p^{n_i}[W_i(a)]$ into J_i is a special case of ring embedding, where elements of finite field are mapped into orthogonal ideals of the same order.

In what follows we consider the mapping ϕ_{ij} as defined by Equation (4.5.5). Though ϕ_{ij} is an isomorphism between the additive abelian group structures of local ring $P_p^{h_i n_i}[W_i^{h_i}(a)]$ and orthogonal ideal J_j , the transformed sequences are orthogonal to each other.

Example 4.5.4

Consider a second order autonomous canonical; $P_2^3[a^3+a+1]$ -LSS, L with characteristic matrix $A_c = \begin{bmatrix} 0 & 1 \\ a & 1 \end{bmatrix}$ and $C = [1 \ 0]$. With initial state $[1 \ 0]^{\text{tr}}$ the output sequence

$$\hat{Z} = (1, 0, a, a, (a^2+a), a, (a^2+1), 1, 0, \dots)$$

Consider semisimple $P_2^6[(a^3+a+1)(a^3+a^2+1)]$.

The orthogonal idempotents in this ring are

$$e_1(a) = (a^4+a^2+a) \quad \text{and} \quad e_2(a) = (a^4+a^2+a+1)$$

Sequence \hat{Z} is transformed into orthogonal sequences $Z^{(1)}$ and $Z^{(2)}$ over $J_1 = \langle e_1(a) \rangle$ and $J_2 = \langle e_2(a) \rangle$ respectively as shown in Figure 4.5.5, the mapping ϕ_i is multiplication by $e_i(a)$ modulo $[2; (a^3+a+1)(a^3+a^2+1)]$; $i = 1, 2$.

$$Z^{(1)} = ((a+a^2+a^4), 0, (a^2+a^3+a^5), (a^2+a^3+a^5), (1+a+a^3), \\ (a^2+a^3+a^5), (1+a^2+a^3+a^4+a^5), (a+a^2+a^4), 0, \dots)$$

$$Z^{(2)} = ((1+a+a^2+a^4), 0, (a+a^2+a^3+a^5), (a+a^2+a^3+a^5), (1+a^2+a^3), \\ (a+a^2+a^3+a^5), (a^2+a^4+a^5), (1+a+a^2+a^4), \dots)$$

$Z^{(1)}$ and $Z^{(2)}$ are orthogonal.

We note here that, ϕ_1 is an isomorphism between the field $P_2^3[a^3+a+1]$ and the orthogonal ideal J_1 and ϕ_2 is an isomorphism between additive abelian group structures of $P_2^3[a^3+a+1]$ and the orthogonal ideal J_2 . However, $Z^{(1)}$ and $Z^{(2)}$ are orthogonal to each other.

Let Z_2^3 -LSS L' be isomorphic to L .

Then sequence $\hat{Z} \simeq \hat{Z}$, and is a sequence of 3-tuples over $Z_2^3 \simeq P_2^3[a^3+a+1]$.

$$\underline{\hat{Z}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

The sequence $\underline{\hat{Z}}$ is transformed into two orthogonal sequences $\underline{Z}^{(1)}$ and $\underline{Z}^{(2)}$ over $Z_2^6 \simeq P_2^6[(a^3+a+1)(a^3+a^2+1)]$.

$$\underline{Z}^{(1)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

$$\underline{Z}^{(2)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \dots$$

We now take up an example, where a sequence over semi-simple ring is transformed into a set of orthogonal sequences over a larger semisimple ring, which contain orthogonal ideals isomorphic to the orthogonal ideals in smaller semisimple ring.

Example 4.5.5

Consider the semisimple ring $P_2^4[a^4+a^2+a]$.

$$W(a) = a(a^3+a+1), W_1(a) = a, W_2(a) = (a^3+a+1).$$

$\overline{W_1}(a) = (a^3+a+1)$, $\overline{W_2}(a) = a$; $\overline{W_1}(a)$ and $\overline{W_2}(a)$ are relatively prime. There exists $b_1(a)$ and $b_2(a)$, which are found by Euclids algorithm [18] such that $\overline{W_1}(a) b_1(a) + \overline{W_2}(a) b_2(a) = e_1(a) + e_2(a) = 1$ modulo $[2; a^4+a^2+a]$. $b_1(a)$ and $b_2(a)$ are found to be 1 and $(1+a^2)$ respectively and the orthogonal idempotents are $e_1(a) = (a^3+a+1)$ and $e_2(a) = (a^3+a)$.

The orthogonal ideals are $J_1 = \langle e_1(a) \rangle = \{0, (1+a+a^3)\} \simeq P_2^1[a]$ and $J_2 = \langle e_2(a) \rangle = \{0, (a+a^4), a, a^2, a^3, (a+a^2), (a^2+a^3), \dots, (a+a^2+a^3)\} \simeq P_2^3[a^3+a+1]$.

An arbitrary sequence over $P_2^4[a^4+a^2+a]$, can be decomposed into two orthogonal sequences over J_1 and J_2 respectively as shown in Figure 4.5.6a.

A set of 4 orthogonal sequences from Z can be generated by embedding the finite fields $P_2^1[a]$ and $P_2^3[a^3+a+1]$ in a larger semisimple ring $P_2^8[a(a+1)(a^3+a+1)(a^3+a^2+1)] = P_2^8[a^8+a]$ which has two orthogonal ideals $\simeq P_2^1[a]$ and two orthogonal ideals $\simeq P_2^3[a^3+a+1]$.

We have $W_1^*(a) = a$, $W_2^*(a) = (a^3+a+1)$, $W_3^*(a) = (a+1)$,

$$W_4^*(a) = (a^3+a^2+1), W^*(a) = (a^8+a)$$

and $\overline{W_1^*}(a) = (a^7+1)$; $\overline{W_2^*}(a) = (a^2+a)(a^3+a^2+1) = (a^5+a^3+a^2+a)$

$$\overline{W_3^*}(a) = (a^7+a^6+a^5+a^4+a^3+a^2+a), \overline{W_4^*}(a) = (a^5+a^3+a^4+a).$$

There exists $b_1(a)$, $b_2(a)$, $b_3(a)$, $b_4(a)$ such that

$$\begin{aligned} & \overline{W_1'(a)} \cdot b_1(a) + \overline{W_2'(a)} \cdot b_2(a) + \overline{W_3'(a)} \cdot b_3(a) + \overline{W_4'(a)} \cdot b_4(a) \\ &= e_1'(a) + e_2'(a) + e_3'(a) + e_4'(a) = 1 \text{ modulo } [2; W(a)]. \end{aligned}$$

By Euclids algorithm [18],

$$\begin{aligned} b_1(a) &= 1 ; b_2(a) = (1+a^2), b_3(a) = 1, b_4(a) = a^2. \text{ Hence,} \\ e_1'(a) &= W_1'(a) \cdot b_1(a) = a^7+1, e_2'(a) = W_2'(a) \cdot b_2(a) = (a^7+a^4+a^2+a) \\ e_3'(a) &= W_3'(a) \cdot b_3(a) = (a^7+a^6+a^5+a^4+a^3+a^2+a) \cdot 1 \text{ and} \\ e_4'(a) &= W_4'(a) \cdot b_4(a) = (a^5+a^4+a^3+a) \cdot a^2 = (a^7+a^6+a^5+a^3). \end{aligned}$$

Transformation of sequence Z over $P_2^4[a^4+a^2+a]$ into a set of four orthogonal sequences over $P_2^8[a^8+a]$ is possible by first decomposing Z into orthogonal sequences $Z^{(1)}$ and $Z^{(2)}$ over J_1 and J_2 respectively. $Z^{(1)}$ and $Z^{(2)}$ are then transformed into two orthogonal sequences each in $P_2^8[a^8+a]$. As shown in figure 4.5.6b, $Z^{(1)}$ is transformed into $Z'^{(1)}$ and $Z'^{(3)}$ over orthogonal ideals $J_1' = \langle e_1(a) \rangle$ and $J_3 = \langle e_3(a) \rangle$ and $Z^{(2)}$ is transformed into $Z'^{(2)}$ and $Z'^{(4)}$ over orthogonal ideals $J_2' = \langle e_2(a) \rangle$ and $J_4' = \langle e_4(a) \rangle$ in $P_2^8[a^8+a]$. The mapping ϕ_i is multiplication by $e_i'(a)$ modulo $P_2^8[a^8+a]$; $i = 1, 2, 3, 4$.

Consider a periodic sequence Z over $P_2^4[a^4+a^2+a]$ generated by a second order nonsingular canonical autonomous $P_2^4[a^4+a^2+a]$ -LSS with $C = [1 \ 0]$ given in Figure 4.5.6c. With the initial state $[1 \ 0]^{\text{tr}}$ the output sequence

$$Z = (1, 0, (1+a), (1+a), (a+a^2), (1+a), (1+a^3), (a^2+a^3), 1, (1+a) \dots)$$

The decomposition of this sequence over $P_2^4[a^4+a^2+a]$ is

$$\begin{aligned} Z^{(1)} &= ((1+a+a^3), 0, (1+a^2+a^3+a^4), (1+a^2+a^3+a^4), (a+a^3+a^4+a^5), \\ &\quad (1+a^2+a^3+a^4), (1+a+a^4+a^6), (a^2+a^4+a^5+a^6), (1+a+a^3), \\ &\quad (1+a^2+a^3+a^4) \dots) \text{ modulo}[2; a^4+a^2+a] \\ &= ((1+a+a^3), 0, (1+a+a^3), (1+a+a^3), 0, (1+a+a^3), 0 \dots) \\ &\quad \text{of period } 3 \end{aligned}$$

$$\begin{aligned} \text{and } Z^{(2)} &= ((a+a^2), 0, (a+a^3), (a+a^3), a, (a+a^3), a, a^2, (a+a^2), \\ &\quad (a+a^3), 0, \dots) \text{ modulo}[2; a^4+a^2+a] \text{ of period } 63. \end{aligned}$$

$Z^{(1)}$ is then transformed into sequences $Z'^{(1)}$ and $Z'^{(3)}$ and $Z^{(2)}$ is transformed into $Z'^{(2)}$ and $Z'^{(4)}$ over $P_2^8[a^8+a]$.

$$Z'^{(1)} = e_1'(a) \cdot Z^{(1)} \text{ modulo}[2; a^8+a]$$

$$Z'^{(3)} = e_3'(a) \cdot Z^{(1)} \text{ modulo}[2; a^8+a]$$

$$Z'^{(2)} = e_2'(a) \cdot Z^{(2)} \text{ modulo}[2; a^8+a]$$

$$Z'^{(4)} = e_4'(a) \cdot Z^{(2)} \text{ modulo}[2; a^8+a]$$

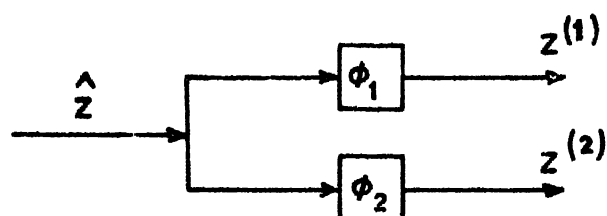


Fig.4.5.5 Transformation of Sequence z into Orthogonal Sequences $z^{(1)}$ and $z^{(2)}$

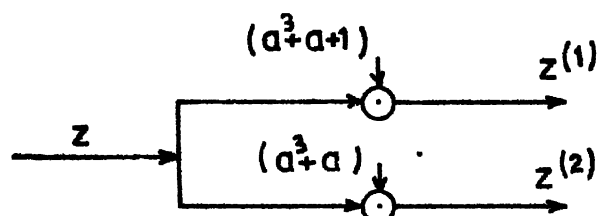
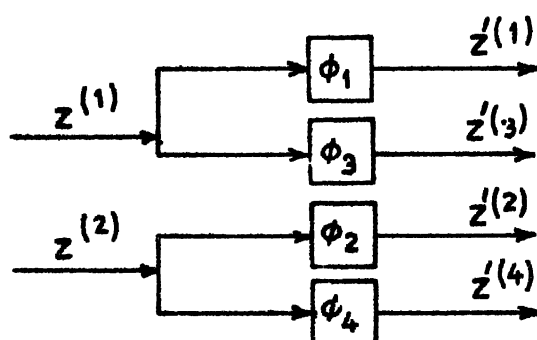


Fig.4.5.6a Decomposition of Sequence z over $P_2^4 [a^4 + a^2 + a]$ of Example 4.5.5



Thus we have,

$$Z^{(1)} = ((1+a^7), 0, (1+a^7), (1+a^7), 0 \dots)$$

$$Z^{(3)} = ((a+a^2+a^3+a^4+a^5+a^6+a^7), 0, (a+a^2+a^3+a^4+a^5+a^6+a^7), \\ (a+a^2+a^3+a^4+a^5+a^6+a^7), \dots)$$

$$Z^{(2)} = ((a+a^4+a^5+a^6), 0, (a+a^2+a^4+a^7), (a+a^2+a^4+a^7), \\ (a+a^2+a^3+a^5), (a+a^2+a^4+a^7), \dots)$$

$$Z^{(4)} = ((a^2+a^4+a^5+a^6), 0, (a^2+a^3+a^4+a^7), (a^2+a^3+a^4+a^7), \\ (a+a^4+a^6+a^7), (a^2+a^3+a^4+a^7), (a+a^4+a^6+a^7) \dots)$$

The elements of sequence Z are polynomials of degree ≤ 4 .

The elements can also be viewed as 4-tuples over $Z_2^4 \simeq P_2^4[a^4+a^2+a]$.

The decomposed orthogonal sequence $Z^{(1)}, Z^{(2)}, Z^{(3)}, Z^{(4)}$

are 8-tuples over $Z_2^8 \simeq P_2^8[a^8+a]$. The procedure for implementation of isomorphic Z_2^4 -LSS and Z_2^8 -LSS is discussed in Chapter 3.

The corresponding sequences are given here.

The sequence \underline{Z} of 4-tuples over $Z_2^4 \simeq P_2^4[a^4+a^2+a]$ is decomposed into orthogonal sequences $\underline{Z}^{(1)}$ and $\underline{Z}^{(2)}$ over Z_2^4 , which is further transformed into orthogonal sequences $\underline{Z}^{(1)}, \underline{Z}^{(2)}, \underline{Z}^{(3)}, \underline{Z}^{(4)}$ of 8-tuples over $Z_2^8 \simeq P_2^8[a^8+a]$. The sequences are

$$\underline{Z} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \dots$$

$$\underline{Z}^{(1)} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \dots$$

$$\underline{Z}^{(2)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \dots$$

$\underline{Z}^{(1)}$ is decomposed into $\underline{Z}'^{(1)}$ and $\underline{Z}'^{(3)}$, and $\underline{Z}^{(2)}$ is decomposed into $\underline{Z}'^{(2)}$ and $\underline{Z}'^{(4)}$ over $\mathbb{Z}_2^8 \simeq \mathbb{P}_2^8[a^8+a]$.

$$\underline{Z}'^{(1)} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \dots$$

$$\underline{z}'^{(3)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} \dots$$

$$\underline{z}'^{(2)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \dots$$

$$\underline{z}'^{(4)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \dots$$

In the next example we consider transformation of sequence over local ring into orthogonal sequences over semilocal ring.

Example 4.5.6

Consider a nonsingular, canonical, single output, autonomous $P_2^2[a^2+1]$ -LSS L with $C = [1 \ 0]$ as shown in Figure 4.5.7a. With the initial state $[1 \ 0]^{\text{tr}}$, the response $Z = (1, 0, a, 1, (1+a), 1, 1, 0, \dots)$ and is of period 6. Z is transformed into two orthogonal sequences $Z^{(1)}$ and $Z^{(2)}$ over the local ring $P_2^4[a^2(a^2+1)] = P_2^4[a^4+a^2]$ as shown in Figure 4.5.7b.

$$w_1^2(a) = a^2, w_2^2(a) = (a^2+1), e_1(a) = (a^2+1), e_2(a) = a^2,$$

and the mapping ϕ_i is multiplication by $e_i(a)$ modulo $[2, a^4+a^2]$;

$$i = 1, 2.$$

$$Z^{(1)} = ((1+a^2), 0, (a+a^3), (1+a^2), (1+a+a^2+a^3), (1+a^2), (1+a^2), 0, \dots)$$

is of period 6 over orthogonal ideal $\langle e_1(a) \rangle$ in $P_2^4[a^4+a^2]$.

$$Z^{(2)} = (a^2, 0, a^3, a^2, (a^2+a^3), a^2, a^2, 0, \dots)$$

is of period 6 over orthogonal ideal $\langle e_2(a) \rangle$ in $P_2^4[a^4+a^2]$.

The corresponding sequences of n -tuples are

\underline{Z} sequence of 2-tuples over $Z_2^2 \simeq P_2^2[a^2+1]$

$\underline{Z}^{(1)}, \underline{Z}^{(2)}$ sequences of 4-tuples over $Z_2^4 \simeq P_2^4[a^2(a^2+1)]$.

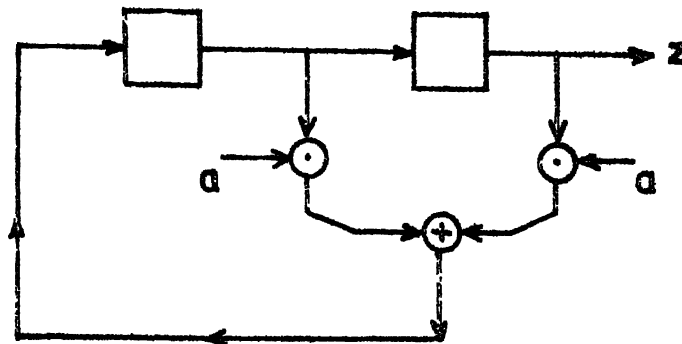


Fig.4.5.7a Generation of Sequence z of Example 4.5.6

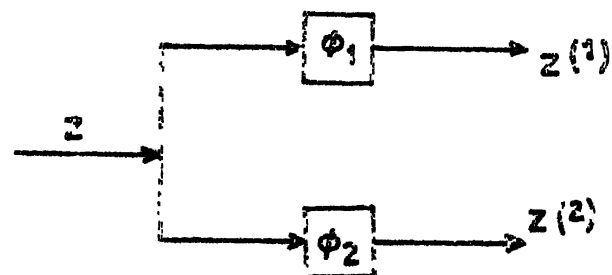


Fig.4.5.7b Transformation of Sequence z into orthogonal sequences $z^{(1)}$ and $z^{(2)}$

$$\underline{Z} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & \dots \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & \dots \end{pmatrix}$$

$$\underline{Z}^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & \dots \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & \dots \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & \dots \end{pmatrix}$$

$$\underline{Z}^{(2)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & \dots \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & \dots \end{pmatrix}$$

4.6 MODULATION AND MULTIPLEXING APPLICATIONS OF SEQUENCES OVER ORTHOGONAL IDEALS

In this section we show that sequences over orthogonal ideals in semisimple rings can be used as carriers which can be modulated by data sequences with elements from finite fields and then multiplexed in a manner analogous to spread spectrum modulation and multiplexing schemes based on pseudonoise binary sequences. In the latter case demultiplexing is done by using the correlation property of the pseudonoise sequences. However, because of finite integration time in the detector, the spread spectrum carriers (P-N sequences) corresponding to undesired data streams are not completely averaged out [79]. Since the

elements of the sequences over distinct orthogonal ideals mutually annihilate, this problem is not present in modulation and multiplexing using orthogonal sequences. Just as in the case of spread spectrum modulation using pseudonoise binary sequences [32,33], the modulation and multiplexing scheme employing sequences over orthogonal ideals has the advantage of selective addressing and inherent message privacy.

We have seen in Section 2.3 that in a semisimple ring $P_p^n[W(a)]$, where $W(a) = \prod_{i=1}^v W_i(a)$; $W_i(a)$ irreducible polynomial of degree n_i over $GF(p)$, the ideal J_i generated by orthogonal idempotent $e_i(a)$ is such that

$$J_i \cong P_p^{n_i}[W_i(a)] \cong GF(p^{n_i}) ; i = 1, 2, \dots, v$$

A K th order canonical single output $P_p^n[W(a)]$ -LSS with $C = [1 \ 0 \ \dots \ 0]$ and coefficients $a_j \in J_i ; j = 1, 2, \dots, K$ can then be obtained such that with the initial values from J_i , the sequence generated is periodic with period $(p^{n_i K} - 1)$. The elements of the sequence are from J_i . This is an example of a singular $P_p^n[W(a)]$ -LSS which generates a periodic sequence for specified initial condition. The sequence so generated is isomorphic to the maximum length $(M-L)$ sequence of period $(p^{n_i K} - 1)$ over finite field $GF(p^{n_i})$.

The $M-L$ sequence over J_i , can be used as a carrier in modulation schemes. A data sequence over $GF(p^{n_i})$ is first transformed to a sequence over J_i by embedding each of its

elements into the ring of higher order which contains orthogonal ideal of order p^{n_i} . The new data sequence over J_i modulates the M-L sequence $Z^{(i)}$ of length $(p^{n_i K} - 1)$ over J_i . If the input to the modulator during a given interval is $r_i(a)$, the sequence generator output is $r_i(a) Z^{(i)}$; that is each element of M-L sequence of length $(p^{n_i K} - 1)$ is multiplied by $r_i(a)$. Thus the data sequence modulates a high rate sequence.

From the result of Lemma 4.5.1, $r_i(a) \cdot r_j(a) = 0$ modulo $[p; W(a)]$ $j = 1, 2, \dots, \nu$, $j \neq i$. The orthogonal property of the elements in the sequence enables us to multiplex the output sequence of ν modulators, each output sequence being over an ideal generated by orthogonal idempotent. Thus in this scheme a data sequence in the i th channel from a source whose elements are from $GF(p^{n_i})$ is transformed to an orthogonal sequence by embedding the sequence elements in $P_p^n[W(a)]$. The resulting sequence which has elements from J_i , modulates the M-L sequence over J_i . The elements of a sequence in a channel are orthogonal to elements in the sequences in the other $(\nu - 1)$ channels. These sequences are added pointwise to obtain a sequence over the ring $P_p^n[W(a)]$ and then transmitted. Because of the orthogonality of the elements in the ideals J_1, J_2, \dots, J_ν , the sequences can be separated at the receiver and the Hamming correlators - the sequence generators of which are time synchronised and phase locked with the transmitter generator - are used to demodulate the received sequence to obtain the data sequence. Only modulation and multiplexing is investigated

here. Noise performance is a topic of further investigation.

The modulation and multiplexing scheme and the corresponding demultiplexing and demodulation scheme are shown in Figures 4.6.1a and 4.6.1b respectively. Source No. i gives out data sequence over $GF(p^{n_i})$. Each element $r_i(a)$ of the data sequence is mapped to a corresponding ring element $r_i(a) \in J_i$ by the mapping ϕ_i , which is multiplication by $e_i(a)$ modulo $[p; W(a)]$. $r_i(a)$ modulates the M-L sequence $Z^{(1)}$ over J_i generated by an autonomous, singular, K_i th order canonical, single output system with initial values from J_i . Since $J_i \cong P_p^{n_i}[W_i(a)] \cong GF(p^{n_i})$, the M-L sequence over J_i is isomorphic to M-L sequence over $GF(p^{n_i})$, whose period is $(p^{n_i K_i} - 1)$. If the input to the modulator is $r_i(a)$ the output of the modulator is $r_i(a) Z^{(i)}$; $i = 1, 2, \dots, \nu$. Thus in the i th channel the input symbols to the modulator are presented at a rate of one symbol per $(p^{n_i K_i} - 1)$ clock duration [when the source alphabet sizes are same that is $n_1 = n_2 = \dots = n_\nu$ and the periods of the modulated sequences are same as $K_1 = K_2 = \dots = K_\nu$], the data rates in the individual channels are same. The number of channels ν is then at most equal to the number of irreducible polynomials of degree n_1 over $GF(p)$.

Since J_i is closed under multiplication the elements in the sequence $r_i(a) Z^{(i)}$ are in J_i . Further since the sequence $Z^{(i)}$ is isomorphic to a M-L sequence over $GF(p^m)$, as we have

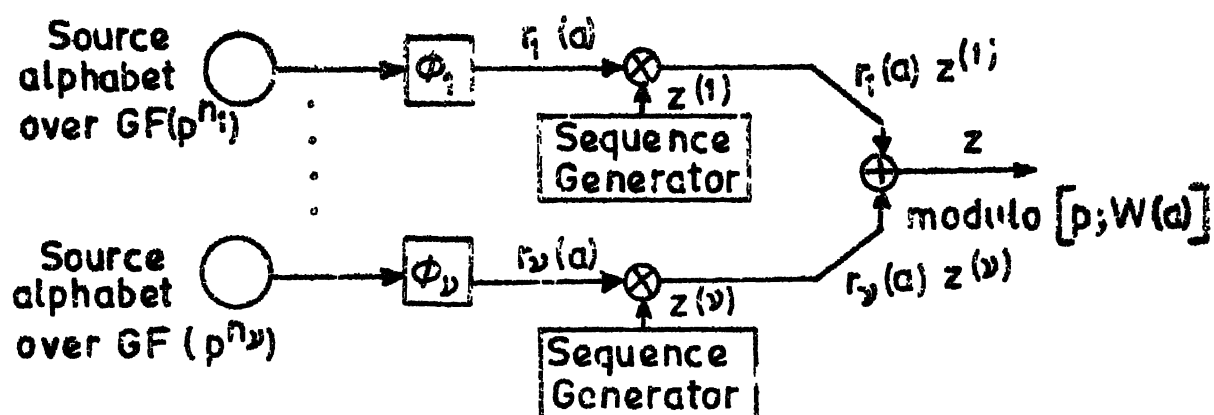


Fig.4.6.1a Modulation and Multiplexing Scheme

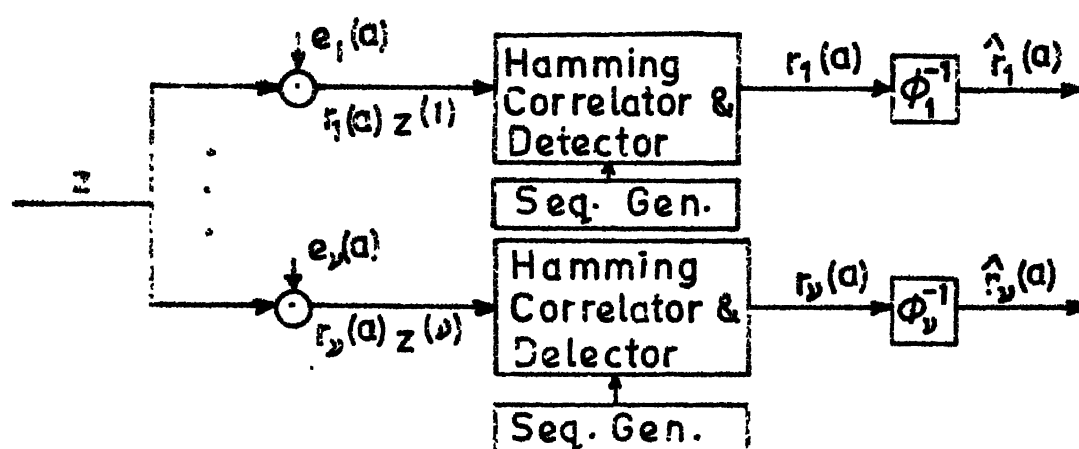


Fig.4.6.1b Demultiplexing and Demodulation Scheme

seen in Section 4.4, $r_i(a) Z^{(i)}$ is a shifted version of $Z^{(i)}$; $i = 1, 2, \dots, \nu$. The elements of the sequence $r_i(a) Z^{(i)}$ are orthogonal to the elements of the sequence in the remaining $(\nu - 1)$ sequences and hence can be multiplexed. The ν sequences are added pointwise modulo $[p; W(a)]$ to get the sequence $Z = r_1(a) Z^{(1)} + r_2(a) Z^{(2)} + \dots + r_\nu(a) Z^{(\nu)}$. As we have seen in Section 2.3, $P_p^n[W(a)]$ is the internal direct sum of ideals J_i , $i = 1, 2, \dots, \nu$. Thus the elements in the sequence Z are the internal direct sum of elements in $r_1(a) Z^{(1)}, \dots, r_\nu(a) Z^{(\nu)}$. Internal direct sum of distinct ordered set of elements from channel $1, 2, \dots, \nu$ give rise to distinct element in $P_p^n[W(a)]$, which is transmitted.

Demultiplexing and demodulation scheme at the receiver is as shown in Fig. 4.6.1b. Demultiplexing is done by multiplying the sequence Z by scalars $e_i(a)$; $i = 1, 2, \dots, \nu$. From the result of the Lemma 4.5.1 we have

$$\begin{aligned} Z \cdot e_i(a) &= r_1(a) Z^{(1)} e_i(a) + \dots + r_i(a) Z^{(i)} e_i(a) + \dots \\ r_\nu(a) Z^{(\nu)} \cdot e_i(a) &= r_i(a) Z^{(i)} \text{ modulo } [p; W(a)], \\ i &= 1, 2, \dots, \nu. \end{aligned}$$

The sequence $r_i(a) Z^{(i)}$ is a shifted version of $Z^{(i)}$ and is cross-correlated with the sequence $Z^{(i)}$. If the sequence is all zero sequence corresponding to $r_i(a) = 0$, the cross-correlator output has only one level of magnitude $(p^{n_i(K_i-1)} - 1)$.

For $r_i(a) = e_i(a)$ the peak of magnitude $(p^{n_i K_i - 1})$ occurs for $\tau = 0$. For other values of $r_i(a)$, as seen from Lemma 4.4.4, the peak occurs at shifts τ equal to a multiple of Θ , where $\Theta = \frac{(p^{n_i K_i} - 1)}{(p^{n_i} - 1)}$. The correlator performs Hamming cross-correlation to obtain the shift τ at which the peak occurs; the detector decides the symbol $r_i(a)$ which has modulated $Z^{(i)}$. ϕ_i^{-1} maps $r_i(a)$ to the corresponding element $r_i(a)$ of the data sequence. $\phi_i^{-1}(r_i(a))$ is obtained by taking $r_i(a)$ modulo $[p; W_i(a)]$.

We now consider a variation of the above scheme. In this scheme given in Figure 4.6.2a and b each element of the data sequence over $GF(p^{n_i})$ in channel i modulates a M-L sequence $\hat{Z}^{(i)}$ over $GF(p^{n_i})$. The modulated M-L sequence say $r_i(a) \hat{Z}^{(i)}$ (which is a shifted version of $Z^{(i)}$) is transformed to a sequence $r_i(a) Z^{(1)}$ over the ideal J_i in $P_p^n[W(a)]$, by the mapping ϕ_i , $i = 1, 2, \dots, \nu$. The ν sequences are then added modulo $[p; W(a)]$ and then transmitted. The transmitted sequence is $Z = r_1(a) Z^{(1)} + \dots + r_\nu(a) Z^{(\nu)}$ modulo $[p; W(a)]$. At the receiver the demultiplexing is done as follows. Sequence elements in $r_i(a) Z^{(i)}$ are multiples of $e_i(a)$. As we have seen in Section 2.3, $e_i(a)$ is a multiple of $\bar{W}_i(a)$; $i = 1, 2, \dots, \nu$. Hence we have,

$$\begin{aligned} Z \text{ modulo } [p; W_i(a)] &= [r_1(a) Z^{(1)} + \dots + r_i(a) Z^{(i)} + \dots \\ &\quad + r_\nu(a) Z^{(\nu)}] \text{ modulo } [p; W(a)]. \\ &= \hat{r}_i(a) \hat{Z}^{(i)} \text{ modulo } [p; W_i(a)]. \end{aligned}$$

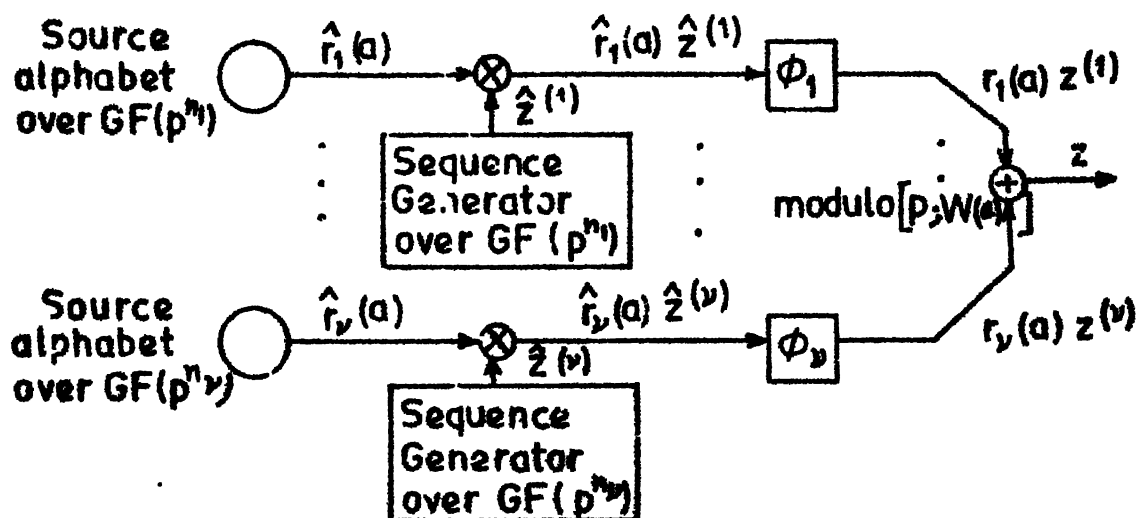


Fig.4.6.2a Alternative Scheme of Modulation and Multiplexing.

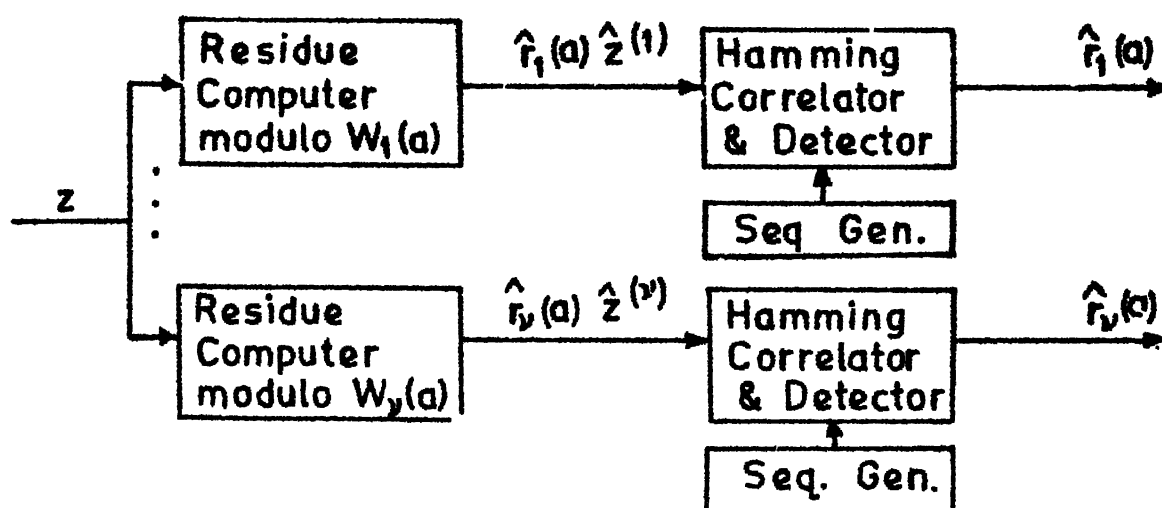


Fig.4.6.2b Alternative Scheme of Demodulation and Demultiplexing

The computation $Z \bmod [p; W_i(a)]$ is carried out by residue computer $\bmod [p; W_i(a)]$ which is a division by $W_i(a)$ circuit which can be implemented by shift registers as discussed in Section 3.1. The remainder which is of interest is the content of the shift register at the end of division operation. $\hat{r}_i(a) \hat{Z}^{(i)}$ is a shifted version of the M-L sequence $\hat{Z}^{(i)}$. As seen in Lemma 4.4.4 the location of the peak value in the Hamming cross-correlation between $\hat{r}_i(a) \hat{Z}^{(1)}$ and $\hat{Z}^{(1)}$ depends on the symbol $\hat{r}_i(a)$; $i = 1, 2, \dots$. The Hamming cross-correlator and detector in the i th channel then gives out the symbol $\hat{r}_i(a)$ which modulated the M-L sequence.

The part of the system between dotted lines 1-1' and 2-2' can be used for multiplexing data sequences over $GF(p^{n_i})$.

In the schemes we have considered, $W(a)$ is a product of irreducible polynomials. In general the degree n_i of $W_i(a)$, $i = 1, 2, \dots$ may be different. The degree of the irreducible factors of $W(a)$ are governed by the alphabet size of the source. If the alphabet size of the sources are different, the length of the modulated sequence in each channel is different. This results in different data rates in each channel. If the clock rates of individual sequence generators are different, for proper mixing of sequences at the multiplexer, the clock rates must be integral multiples of the lowest rate sequence generator. The number of channels that can be multiplexed is equal to the number of irreducible

factors of $W(a)$. If the sources are of same alphabet size that is $n_1 = n_2 = \dots = n_\nu$ and the periods of the modulated sequences are same ^{i.e} $K_1 = K_2 = \dots = K_\nu$, the data rates in the individual channels are same. The number of channels ν is then at most equal to the number of irreducible polynomials of degree n_1 over $GF(p)$. From the consideration of number of memory devices required, the second scheme requires less number compared to the first scheme.

In the following we give a comprehensive example to illustrate the technique of modulation and multiplexing of orthogonal sequences. We consider sources of different alphabet size. The alphabet size is assumed to be power of a prime p . Given an alphabet size the number of sources which can be multiplexed, is atmost equal to the number of irreducible polynomials of appropriate degree.

Example 4.6.1

Suppose data sequence from three sources are to be multiplexed. Let the alphabet size of two sources S_1 and S_2 be 2 and that of source S_3 be 4.

We choose

$$W_1(a) = a,$$

$$W_2(a) = (a+1),$$

$$W_3(a) = (a^2+a+1), \text{ over } GF(2)$$

$$W(a) = (a^4+a)$$

and the ring is $P_2^4[a^4+a]$.

As defined in Section 2.3,

$$\overline{w_1(a)} = w_2(a) \cdot w_3(a) = (a^3+1)$$

$$\overline{w_2(a)} = w_1(a) \cdot w_3(a) = (a^3+a^2+a)$$

$$\overline{w_3(a)} = w_1(a) \cdot w_2(a) = (a^2+a)$$

We see that $(a^3+1) \cdot 1 + (a^3+a^2+a) \cdot 1 + (a^2+a) \cdot 1 = 1$ modulo $[2; a^4+a]$.

Hence the orthogonal idempotents are

$$e_1(a) = (a^3+1)$$

$$e_2(a) = (a^3+a^2+a)$$

$$e_3(a) = (a^2+a)$$

$$J_1 = \langle e_1(a) \rangle = \{0, (1+a^3)\} \simeq P_2^1(a) \simeq GF(2)$$

$$J_2 = \langle e_2(a) \rangle = \{0, (a+a^2+a^3)\} \simeq P_2^1[a+1] \simeq GF(2)$$

$$J_3 = \langle e_3(a) \rangle = \{0, (a+a^2), (a^2+a^3), (a+a^3)\} \simeq P_2^2[a^2+a+1]$$

Scheme 1

Source generators : The period of the sequences from the three generators need not be same. The orthogonality of the sequences are still maintained. Sequence $Z^{(1)}$ over J_1 : We

consider a 2nd order, canonical, single output LSS over J_1 with $C = [1, 0]$ and characteristic matrix $A_c = \begin{bmatrix} 0 & 1 \\ 1+a^3 & 1+a^3 \end{bmatrix}$.

The sequence $Z^{(1)}$ with initial state $[0, 1+a^3]^{tr}$ is an M-L sequence of period 3 over J_1

$$Z^{(1)} = ((1+a^3), 0, (1+a^3), (1+a^3), 0, (1+a^3), \dots)$$

Sequence $Z^{(2)}$ over J_2 : We consider a 2nd order canonical, single output LSS over J_2 with $C = [1, 0]$ and characteristic matrix $A_c = \begin{bmatrix} 0 & 1 \\ a+a^2+a^3 & a+a^2+a^3 \end{bmatrix}$. The sequence $Z^{(2)}$ with initial value $[0, (a+a^2+a^3)]^{tr}$ is an M-L sequence of period 3 over J_2

$$Z^{(2)} = ((a+a^2+a^3), 0, (a+a^2+a^3), (a+a^2+a^3), \dots)$$

Sequence $Z^{(3)}$ over J_3 : We consider a 2nd order canonical single output LSS over J_2 with $C = [1, 0]$ and characteristic matrix $A_c = \begin{bmatrix} 0 & 1 \\ a+a^3 & a+a^3 \end{bmatrix}$. The sequence $Z^{(3)}$ with initial value $[0, (a+a^3)]^{tr}$ is

$$Z^{(3)} = ((a+a^3), 0, (a^2+a^3), (a+a^2), (a^2+a^3), (a^2+a^3), \dots)$$

The sequence is of length $(2^4-1) = 15$

$$Z^{(3)} = (\bar{Z}^{(3)}, (a+a^3) \bar{Z}^{(3)}, (a^2+a^3) \bar{Z}^{(3)} \dots)$$

where $\bar{Z}^{(3)}$ is a segment of length 5 of sequence $Z^{(3)}$.

The modulation and multiplexing scheme is given in Figure 4.6.3a.

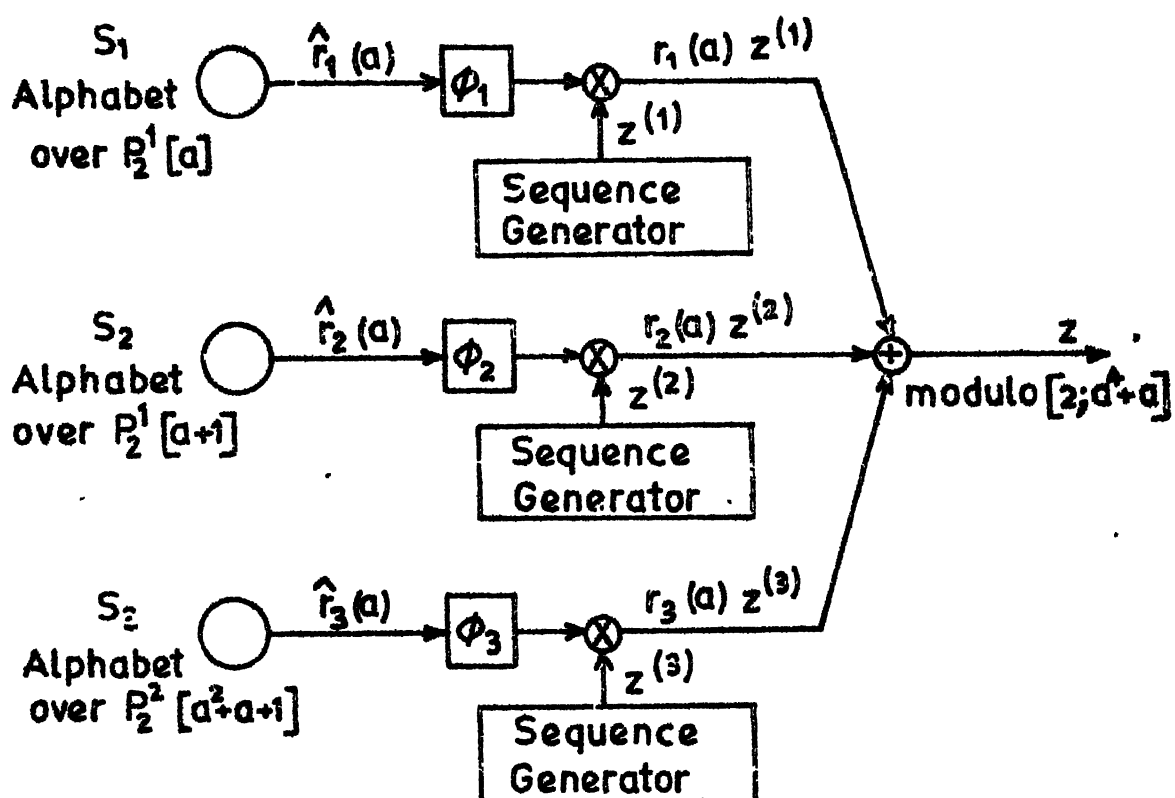


Fig.4.6.3a Modulation and Multiplexing Scheme of System of Example 4.6.1

Suppose the input from source S_1 is $\hat{r}_1(a) = 1 \in P_2^1[a]$
 from source S_2 is $\hat{r}_2(a) = 0 \in P_2^1[a+1]$ and from source
 S_3 is $\hat{r}_3(a) = (1+a) \in P_2^2[a^2+a+1]$.

The corresponding elements in orthogonal ideals are

$$r_1(a) = (1+a^3) \in J_1, \quad r_2(a) = 0 \in J_2, \quad r_3(a) = (a+a^3) \in J_3 \text{ and}$$

$$r_1(a) Z^{(1)} = ((1+a^3), 0, (1+a^3), (1+a^3), 0, (1+a^3) \dots)$$

$$r_2(a) Z^{(2)} = (0, 0, 0, \dots)$$

$$r_3(a) Z^{(3)} = ((a^2+a^3), 0, (a+a^2), (a+a^3), (a+a^2), (a+a^2), 0, \dots)$$

$r_3(a) Z^{(3)}$ is $\sigma^{10} Z^{(3)}$, that is a shifted version- of $Z^{(3)}$.

The transmitted sequence is

$$Z = r_1(a) Z^{(1)} + r_2(a) Z^{(2)} + r_3(a) Z^{(3)}$$

$$= ((1+a^2), 0, (1+a+a^2+a^3), (1+a), (a+a^2), (1+a+a^2+a^3), 0, \dots)$$

Demultiplexing and demodulation scheme is given in

Figure 4.6.3b.

$$r_1(a) Z^{(1)} = e_1(a) Z \text{ modulo}[2; a^4+a]$$

$$= ((1+a^3), 0, (1+a^3), (1+a^3), 0, \dots)$$

Correlator output peak occurs at $\tau = 0$. Hence $r_1(a) = (1+a^3)$

$$r_2(a) Z^{(2)} = e_2(a) \cdot Z \text{ modulo}[2, a^4+a] = (0, 0, 0, \dots)$$

Correlator output does not have a peak. Hence $r_2(a) = 0$

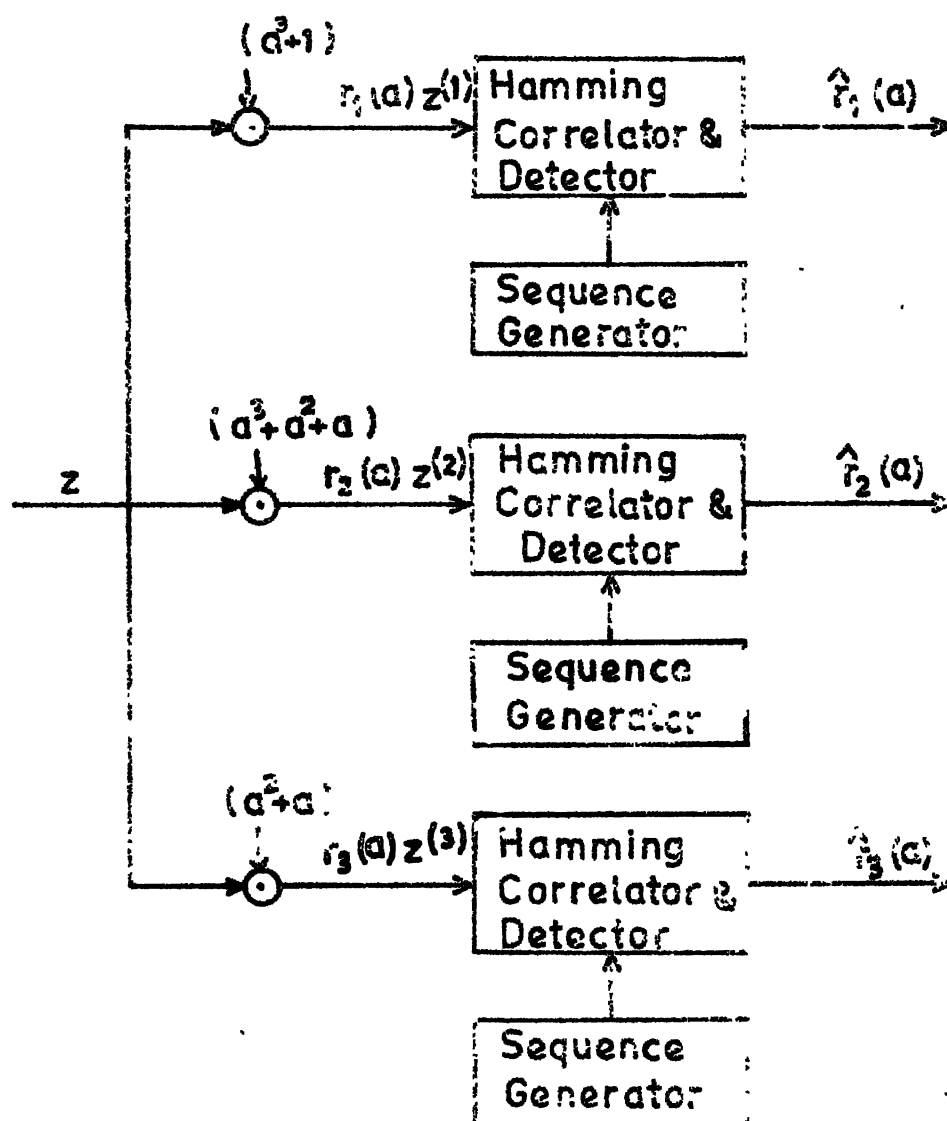


Fig.4.6.3b Demultiplexing and Demodulation of $r_1(a)$ of System of Example 4.2.

$$r_3(a) Z^{(3)} = e_3(a) \cdot Z \text{ modulo}[2; a^4+a]$$

$$= ((a^2+a^3), 0, (a+a^2), (a+a^3), (a+a^2), \dots)$$

$r_3(a) Z^{(3)} = \sigma^{10} Z^{(3)}$ is a shifted version of $Z^{(3)}$.

Length of segment of sequence $Z^{(3)}$ is $\Theta = 5$ and period of $Z^{(3)}$ is $15 = 3\Theta$ and correlator peak occurs at $\tau = 10 = 2\Theta$.

$$Z^{(3)} = (\bar{Z}^{(3)}, (a+a^3)\bar{Z}^{(3)}, (a^2+a^3)\bar{Z}^{(3)} \dots)$$

Hence from Lemma 4.4.4, $r_3(a) = (a+a^3)^j$ where

$$j = \left(\frac{3\Theta-2\Theta}{\Theta}\right) = 1.$$

$$\hat{r}_1(a) = r_1(a) \text{ modulo}[2; a] = 1$$

$$\hat{r}_2(a) = r_2(a) \text{ modulo}[2; [a+1]] = 0 \text{ and } \hat{r}_3(a) =$$

$$r_3(a) \text{ modulo}[2; a^2+a+1] = (1+a).$$

Scheme 2

We consider the alternative schemes given in Figures 4.6.4a and 4.6.4b.

The sequences $\hat{Z}^{(1)}$, $\hat{Z}^{(2)}$ and $\hat{Z}^{(3)}$ are generated as follows :

Sequence $\hat{Z}^{(1)}$ and $\hat{Z}^{(2)}$: Response of 2nd order canonical single output $P_2^1[a]$ -LSS with characteristic matrix

$$A_c = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \text{ and } C = [1 \ 0]. \text{ With initial state } [1 \ 0]^{\text{tr}}$$

the output sequence $\hat{Z}^{(1)} = (1 \ 0 \ 1 \ 1 \ 0 \ 1 \dots)$ and an identical generator generates, $\hat{Z}^{(2)} = (1 \ 0 \ 1 \ 1 \ 0 \ 1 \dots)$.

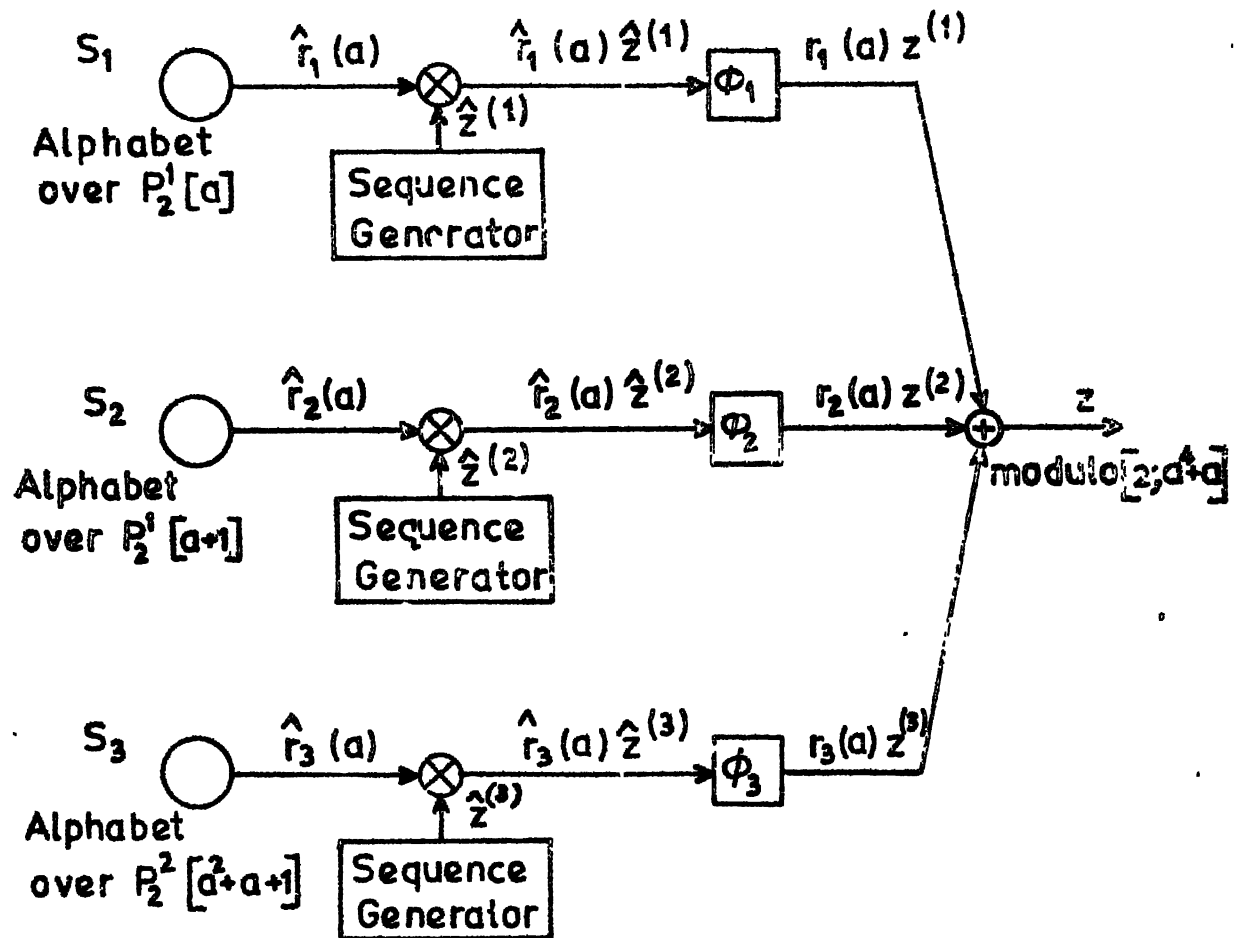


Fig.4.6.4a Alternative Modulation and Multiplexing Scheme of System of Example 4.6.1

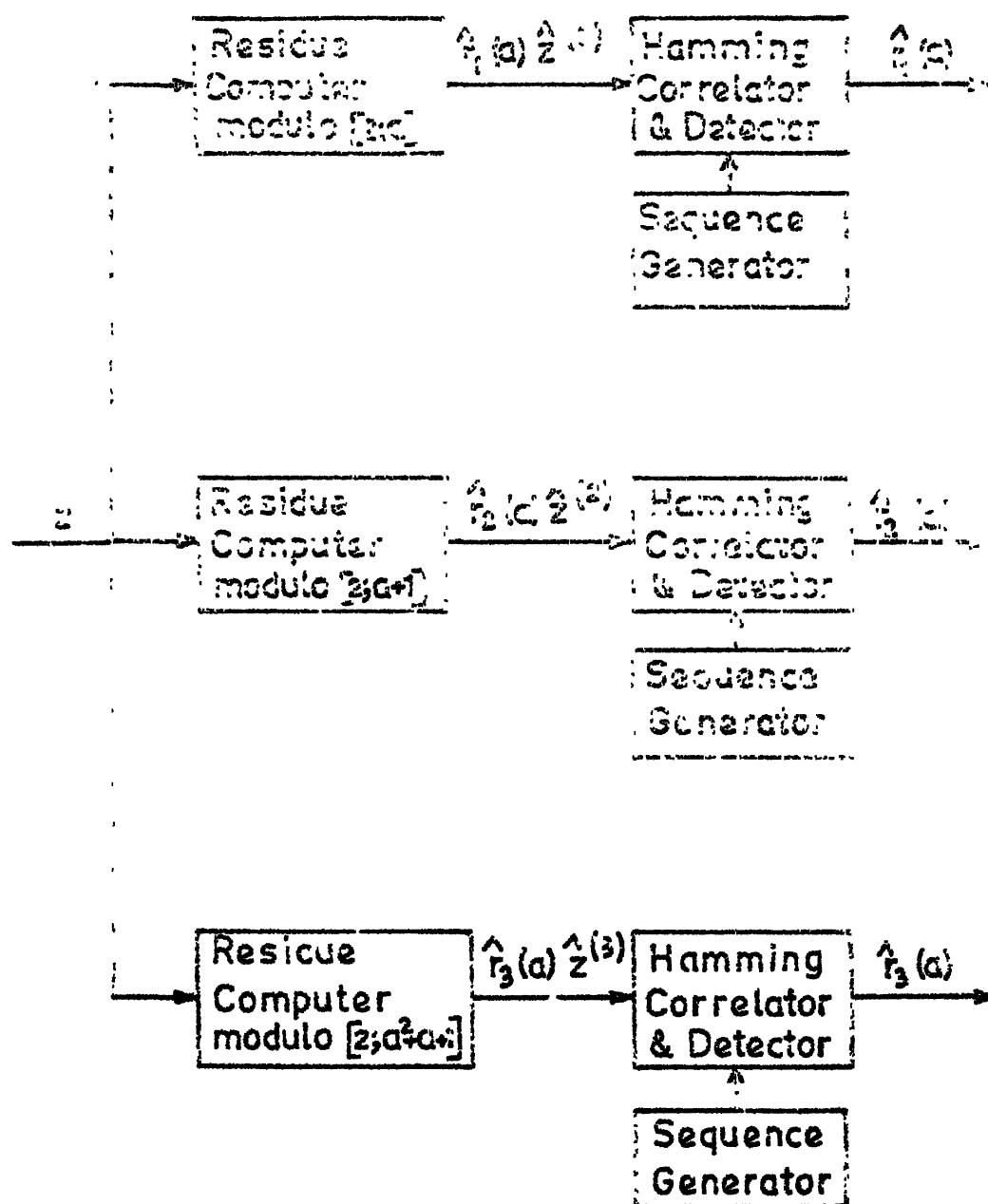


Fig. 4.6-4b Demultiplexing and Demodulation Scheme of System of Example 4.6.1

Sequence $Z^{(3)}$: Response of 2nd order canonical single output

$P_2^2[a^2+a+1]$ -LSS with characteristic matrix $A_c = \begin{bmatrix} 0 & 1 \\ 1+a & 1+a \end{bmatrix}$

and $C = [1 \ 0]$. With initial state $[1+a, 0]^{\text{tr}}$ we have

$$\hat{Z}^{(3)} = ((1+a), 0, a, 1, a, a, 0, 1, (1+a), 1, \dots)$$

Let $\hat{r}_1(a) = 1 \in P_2^1(a)$; $\hat{r}_2(a) = 0 \in P_2^1[a+1]$ and

$$\hat{r}_3(a) = (1+a) \in P_2^2[a^2+a+1].$$

$$\hat{r}_1(a) \hat{Z}^{(1)} = (1, 0, 1, 1, 0, 1, \dots) \text{ over } P_2^1[a]$$

$$\hat{r}_2(a) \hat{Z}^{(2)} = (0, 0, \dots) \text{ over } P_2^1[a+1]$$

$$\hat{r}_3(a) \hat{Z}^{(3)} = (a, 0, 1, 1+a, 1, 1, 0, 1+a, \dots) \text{ over } P_2^2[a^2+a+1].$$

With multiplication modulo $[2; a^4+a]$

$$r_1(a) Z^{(1)} = e_1(a) \hat{r}_1(a) \hat{Z}^{(1)} = ((1+a^3), 0, (1+a^3), 0, \dots)$$

$$r_2(a) Z^{(2)} = e_2(a) \hat{r}_2(a) \hat{Z}^{(2)} = (0, 0, 0, \dots)$$

$$r_3(a) Z^{(3)} = e_3(a) \hat{r}_3(a) \hat{Z}^{(3)} = ((a^2+a^3), 0, (a+a^2), (a+a^3), (a+a^2), (a+a^2), \dots)$$

$$\begin{aligned} Z &= r_1(a) Z^{(1)} + r_2(a) Z^{(2)} + r_3(a) Z^{(3)} = \\ &((1+a^2), 0, (1+a^2+a^2+a^3), (1+a), (a+a^2), \\ &(1+a+a^2+a^3), \dots) \end{aligned}$$

At the receiver the three residue computers generate $\hat{r}_1(a) \hat{z}^{(1)}$, $\hat{r}_2(a) \hat{z}^{(2)}$ and $\hat{r}_3(a) \hat{z}^{(3)}$ respectively.

$$\hat{r}_1(a) \hat{z}^{(1)} = Z \text{ modulo}[2; a] = (1, 0, 1, 1, 0, 1, \dots)$$

$$\hat{r}_2(a) \hat{z}^{(2)} = Z \text{ modulo}[2; a+1] = (0, 0, 0, \dots)$$

$$\hat{r}_3(a) \hat{z}^{(3)} = Z \text{ modulo}[2; a^2+a+1] = (a, 0, 1, (1+a), 1, 1, \dots)$$

The correlator outputs are $\hat{r}_1(a) = 1$, $\hat{r}_2(a) = 0$

and $\hat{r}_3(a) \hat{z}^{(3)} = \sigma^{10} \hat{z}^{(3)}$ is a shifted version of $\hat{z}^{(3)}$. Since the shift is $\tau = 10 = 2\theta$ the peak occurs at $\tau = 10 = 2\theta$; period of sequence is $15 = 3\theta$. Hence from Lemma 4.4.4,

$$\hat{r}_3(a) = (1+a)^j \text{ where } j = \frac{3\theta - 2\theta}{\theta} = 1.$$

Using the isomorphism between Z_2^n and $P_2^n[W(a)]$ the modulated sequence in each channel and the multiplexed sequence can alternatively be viewed as appropriate n-tuples over GF(2). These sequences are denoted by respective symbols with under bar.

Scheme 1

Sequence are over $Z_2^4 \simeq P_2^4[a^4+a]$

$$\underline{z}^{(1)} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \dots$$

$$\underline{z}^{(2)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} \dots$$

$$\underline{z}^{(3)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \dots$$

$$\hat{\underline{r}}_1(a) = 1 ; \quad \hat{\underline{r}}_2(a) = 0 ; \quad \hat{\underline{r}}_3(a) = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\underline{r}_1(a) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} ; \quad \underline{r}_2(a) = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} ; \quad \underline{r}_3(a) = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

$$\underline{r}_1(a) \underline{z}^{(1)} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} \dots$$

$$\underline{r}_2(a) \underline{z}^{(2)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \dots$$

$$\underline{r}_3(a) \cdot \underline{z}^{(3)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & \dots \\ 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

The transmitted sequence is

$$\begin{aligned} \underline{z} &= \underline{r}_1(a) \underline{z}^{(1)} + \underline{r}_2(a) \cdot \underline{z}^{(2)} + \underline{r}_3(a) \cdot \underline{z}^{(3)} \\ &= \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & \dots \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Demultiplexing separates the sequences and correlator gives out the symbols $\hat{\underline{r}}_1(a)$, $\hat{\underline{r}}_2(a)$, $\hat{\underline{r}}_3(a)$ in the respective channels.

Scheme 2

$$\hat{\underline{z}}^{(1)} = (1 \ 0 \ 1 \ 1 \ 0 \ 1 \ \dots) \quad \text{over GF}(2)$$

$$\hat{\underline{z}}^{(2)} = (1 \ 0 \ 1 \ 1 \ 0 \ 1 \ \dots) \quad \text{over GF}(2)$$

$$\hat{\underline{z}}^3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & \dots \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & \dots \end{pmatrix} \quad \text{over GF}(2^2)$$

$$\hat{\underline{r}}_1(a) = 1, \hat{\underline{r}}_2(a) = 0, \hat{\underline{r}}_3(a) = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \text{as before.}$$

$$\hat{\underline{r}}_1(a) \hat{\underline{z}}^{(1)} = (1 \ 0 \ 1 \ 1 \ 0 \ 1 \ \dots) \quad \text{over GF}(2)$$

$$\hat{\underline{r}}_2(a) \hat{\underline{z}}^{(2)} = (0 \ 0 \ 0 \ \dots) \quad \text{over GF}(2)$$

$$\hat{\underline{r}}_3(a) \hat{\underline{z}}^{(3)} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & \dots \end{pmatrix} \quad \text{over GF}(2^2).$$

$$\underline{e}_1(a) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} ; \quad \underline{e}_2(a) = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} ; \quad \underline{e}_3(a) = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} .$$

$$\begin{aligned} \underline{r}_1(a) \underline{z}^{(1)} &= \underline{e}_1(a) \hat{\underline{r}}_1(a) \hat{\underline{z}}^{(1)} \\ &= \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot \hat{\underline{z}}^{(1)} = \begin{pmatrix} 1 & 0 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 1 & 1 & \dots \end{pmatrix} \\ \underline{r}_2(a) \underline{z}^{(2)} &= \underline{e}_2(a) \hat{\underline{r}}_2(a) \hat{\underline{z}}^{(2)} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot \hat{\underline{z}}^{(2)} = \begin{pmatrix} 0 & 0 & \dots \\ 0 & 0 & \dots \\ 0 & 0 & \dots \\ 0 & 0 & \dots \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \underline{r}_3(a) \underline{z}^{(3)} &= \underline{e}_3(a) \hat{\underline{r}}_3(a) \hat{\underline{z}}^{(3)} \\ &= \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \cdot \hat{\underline{z}}^{(3)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 1 & 1 & 1 & \dots \\ 1 & 0 & 1 & 0 & 1 & 1 & \dots \\ 1 & 0 & 0 & 1 & 0 & 0 & \dots \end{pmatrix} \end{aligned}$$

As before the transmitted sequence is \underline{z} . At the receiver the three residue computers generate $\hat{\underline{r}}_1(a) \hat{\underline{z}}^{(1)}$, $\hat{\underline{r}}_2(a) \hat{\underline{z}}^{(2)}$ and $\hat{\underline{r}}_3(a) \hat{\underline{z}}^{(3)}$ respectively and the correlator outputs in the respective channels give the data symbol.

The modulation and multiplexing schemes discussed in this section have inherent message privacy since the data sequences are in coded form. Sequences and orthogonal ideals can also be

used for selective addressing, in which a single transmitter makes contact with any one of the several receivers by proper choice of sequences. Each receiver is assigned a particular code sequence over a particular orthogonal ideal. With different code sequences over different orthogonal ideals, assigned to all of the receivers in a network, a transmitter can select any one receiver for communication by transmitting the code sequence corresponding to that receiver.

CHAPTER 5

APPLICATION TO ERROR CONTROL CODING

In this chapter we study linear block codes over $P_p^n[W(a)]$ on lines similar to linear block codes over finite fields [12,17-21] and show how $P_p^n[W(a)]$ -LSS can be utilised for encoding and decoding of polynomial and cyclic codes over $P_p^n[W(a)]$.

Consider blocks of length n in a sequence of symbols from $GF(p)$. We can define a mapping of K such blocks to N blocks i.e. a mapping of nK tuples to nN tuples over $GF(p)$, resulting in an (nN, nK) block code over $GF(p)$. As seen in Section 2.6 there is a one to one correspondence between elements of $P_p^n[W(a)]$ and n -tuples over $GF(p)$. Therefore, the (nN, nK) block code over $GF(p)$ can alternatively be viewed and studied as an (N, K) block code over $P_p^n[W(a)]$. The results of the study over $P_p^n[W(a)]$ can then be taken over to (nN, nK) block code over $GF(p)$. When $W(a)$ is irreducible over $GF(p)$, $P_p^n[W(a)]$ becomes $GF(p^n)$ and codes over $GF(p^n)$ can be looked upon as a special case of codes over $P_p^n[W(a)]$.

In Section 5.1 we briefly review the coding problem in the context of (N, K) block codes over an arbitrary alphabet of finite size. Section 5.2 deals with linear block codes over $P_p^n[W(a)]$ which are characterised by generator matrix G or

parity check matrix H ; the elements of G and H are from $P_p^n[W(a)]$. Restrictions on the choice of H due to the presence of zero divisors in $P_p^n[W(a)]$ have been discussed. The relation between minimum Hamming distance of linear block codes and their error correcting capability, and decoding procedure using decoding table are given.

A specific class of linear block codes namely (N, K) polynomial codes over $P_p^n[W(a)]$ are studied in Section 5.3. In such codes every code word expressed as a polynomial $y(x)$, is a multiple of a fixed polynomial $g(x)$ of degree $(N-K)$ over $P_p^n[W(a)]$; this fixed polynomial is called the generating polynomial. It is shown that for $g(x)$ to be a generating polynomial of the code, either the constant term g_0 or the coefficient of highest degree term g_{N-K} must be a unit in $P_p^n[W(a)]$. Encoding principles, minimum distance properties and decoding principles for systematic and nonsystematic polynomial codes are given.

A subclass of polynomial codes namely (N, K) linear cyclic codes over $P_p^n[W(a)]$ are studied in Section 5.4. In a cyclic code cyclic shift of every code word is also a code word. It is shown that for the case when the generating polynomial $g(x)$ divides $(x^N - 1)$, the polynomial code generated by $g(x)$, becomes a cyclic code. Encoding principles, minimum distance properties and decoding principles for systematic and nonsystematic

cyclic codes are given. Cyclic codes can be decoded in the same manner as polynomial codes. Other decoding principles considered are the permutation decoding similar to that of the systematic cyclic codes over finite fields [54] and the Hamming cross correlation method.

Implementation aspects of encoders for (N,K) polynomial and cyclic codes over $P_p^n[W(a)]$ are presented in Section 5.5. Three encoder structures are suggested. Encoder No. 1 is basically a feedforward $P_p^n[W(a)]$ -LSS which performs polynomial multiplication and generates nonsystematic polynomial or cyclic code. Encoder No.2 generates systematic polynomial or cyclic code. It is basically a LSS which performs polynomial division by $g(x)$ to generate the check symbols. Encoder No.3 is a nonsingular autonomous LSS whose autonomous responses of one periodic length constitute a systematic cyclic code. Interleaving of code words is done to combat long bursts of errors. Encoder structures for interleaved codes over $P_p^n[W(a)]$ are given. Using the isomorphism between $P_p^n[W(a)]$ and $Z_p^n[W]$ as given in Section 2.6 all the above encoders can be implemented over $GF(p)$. The message and codeword symbols then correspond to n -tuples over $GF(p)$. The operations of addition and multiplication of n -tuples in the encoder take place in parallel fashion. However, when the code is over the ring $P_p^n[a^n-1]$, the operations of addition and multiplication can be implemented serially. The hardware needed for serial operation is less than

that required for codes over the general $P_p^n[W(a)]$ which includes codes over $GF(p^n)$ such as given in [80].

Decoder structures for polynomial and cyclic codes over $P_p^n[W(a)]$ are considered in Section 5.6. Three decoders are given. In the first one the decoding is based on syndrome calculation using polynomial division circuit suitable for both systematic and nonsystematic polynomial and cyclic codes. The second decoder is based on the Hamming cross correlation property of systematic and nonsystematic cyclic codes. The third decoder is the permutation decoder for decoding systematic cyclic codes.

5.1 CODING PROBLEM

When we wish to transmit a sequence of symbols from a finite alphabet over a noisy channel the channel noise will occasionally cause a transmitted symbol to be received as another symbol. This undesirable feature of channel though cannot be prevented its effect can be reduced by the use of coding.

In block coding a sequence of K message symbols is transformed (encoded) into a block of $N = K+r$ symbols. The sequence of N symbols which the encoder transmits is called a codeword. If the size of the symbol alphabet is q then q^N sequences of length N are possible out of which only q^K are codewords. The set of all codewords is called an (N,K) block code.

The ratio K/N in an (N,K) block code is called the rate of the code. It is desirable to have as high a rate as possible for the efficient use of channel.

The number of nonzero symbols in a codeword is called its Hamming weight or simply weight. The set of weights w of codewords and the corresponding number $Q(w)$ of codewords constitute the weight structure $\{w_1, Q(w)\}$ of the code. The number of locations at which the symbols of two codewords differ is called the Hamming distance between the codewords. The least of all possible Hamming distances in a code is called the minimum distance of the code.

The noise associated with the channel can be regarded as an independent sequence of symbols of length N which is added component wise to the transmitted codeword. Because of noise the received word may be anyone of the q^N words of length N symbols. The difference between the transmitted codeword and the received word is called error word. The weight of an error word is equal to the number of places at which it changes the symbols in the codeword. When the received word is not a codeword an acknowledgement that an error has occurred, is called error detection. From the received word, determining the most likely transmitted word is called error correction. Only those error words which are not codewords may be detected and corrected.

Error detection/correction capability of a block depends on its minimum distance. In the next section we shall see that greater the minimum distance better the error detecting and correcting capability.

A code which can correct all patterns of t or less errors is called a t error correcting code. A necessary condition for a t error correcting (N,K) block code containing M codewords with symbols from an alphabet size q is

$$\sum_{i=0}^t M(q-1)^i \binom{N}{i} \leq q^N, \quad (5.1.1)$$

called the Hamming bound [18-20].

With $M = q^K$, (5.1.1) becomes

$$\sum_{i=0}^t (q-1)^i \binom{N}{i} \leq q^{(N-K)} \quad (5.1.2)$$

A code is said to be perfect or close packed if it satisfies Expression (5.1.1) with equality for some t and it can correct all errors of weight less than or equal to t and no error of greater weight. The existence of single error correcting perfect codes over finite fields is established [81] and single error correcting. Hamming codes over commutative ring of residue class integers modulo $m = p^h$ are given in [48]. However, these codes are not perfect unless $h = 1$.

If the errors are within the error detecting/correcting capability of the code then from the N received symbols it is possible to detect/correct the errors introduced by the channel. The error detection/correction is done by the decoder whose structure depends on the criterion used for the error detection/correction.

Two decoder structures are possible. A decoder may either minimise the probability of error or maximise the likelihood of the received word. The latter one is called the maximum likelihood decoder. If it is assumed that the message words are equiprobable then the two decoders are equivalent. Further if it is assumed that the message symbols are equiprobable, then maximum likelihood decoding is equivalent to minimum distance decoding. The decoding rule then becomes : find the codeword nearest to the received word in the Hamming distance sense. If more than one codeword are nearest to the received word, choose any one of them.

The main problem in coding theory is to find codes with large rate for efficiency and large minimum distance to correct many errors. These are conflicting goals and in general it is difficult to obtain codes meeting both requirements simultaneously. A way of tackling this situation is to consider various classes of codes and choose the ones having the desired properties. From the practical point of view simpler encoder and

decoder schemes are desired. Hence codes can also be chosen from this point of view by imposing appropriate constraints on the codewords.

With this as background we now study linear block codes over $P_p^n[W(a)]$.

5.2 LINEAR BLOCK CODES OVER $P_p^n[W(a)]$

Consider an (N, K) block code over $P_p^n[W(a)]$; since the degree of $W(a)$ is n , the order of $P_p^n[W(a)]$ is p^n . The set, say, V of all p^{nN} N -tuples over $P_p^n[W(a)]$, constitutes a free $P_p^n[W(a)]$ -module of rank N .

A linear block code over $P_p^n[W(a)]$ is a set of codewords (N -tuples) which is closed under addition and scalar multiplication; the scalars being drawn from $P_p^n[W(a)]$. In other words a linear block code over $P_p^n[W(a)]$ constitutes a submodule of V . Consider free submodules of rank K of the module V . The order of such a submodule is less than or equal to p^{nK} . Since the number of message words for a given K is p^{nK} , for a one-to-one correspondence between message and codewords, the order of C (number of codewords in C), must be p^{nK} . Hence our interest is in those free submodules of rank K whose order is p^{nK} . Thus a linear (N, K) block code C over $P_p^n[W(a)]$ is a free submodule of rank K and order p^{nK} , of the $P_p^n[W(a)]$ -module V .

Example 5.2.1 : Consider the residue class polynomial ring $P_2^2[a^2+1]$. This ring is of order 4 and the set V of all 3-tuples over it constitutes a free module of rank 3 and order $4^3 = 64$.

Consider the following submodule of 3-tuples in V .

$\{(0\ 0\ 0)\ ((1+a)\ (1+a)\ (1+a))\}$. This is a submodule of rank 1 and order $2 < (2^2)^1$. Therefore, it does not constitute a linear block code.

Consider the submodule C

$\{(0\ 0\ 0)\ (1\ 1\ 1)\ (a\ a\ a)\ ((1+a)\ (1+a)\ (1+a))\}$.

The order and rank of this submodule are 4 and 1 respectively and the element $(1\ 1\ 1)$ constitutes a basis of this submodule; other elements in C can be expressed as a multiple of $(1\ 1\ 1)$. C is therefore a $(3,1)$ linear block code. Table 5.2.1 gives one possible mapping of message words to codewords of the $(3,1)$ linear block code C . The table also gives codes over Z_2^2 which is based on the isomorphism between Z_2^2 and $P_2^2[a^2+1]$.

The $(3,1)$ linear block code C considered in this example is a repetition code where each message symbol is repeated 3 times out of which 2 symbols constitute the parity check symbols.

*

Since C is a free submodule of rank K and order p^{nK} , any set of K linearly independent codewords constitutes a basis

Table 5.2.1

$(3,1)$ linear block code over $P_2^2[a^2+1]$ and
 $Z_2^2 \cong P_2^2[a^2+1]$ of Example 5.2.1

$P_2^2[a^2+1]$				Z_2^2			
u	y			u	y		
0	(0	0	0)	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
1	(1	1	1)	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
a	(a	a	a)	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
1+a	((1+a	(1+a	(1+a))	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

and any codeword is a linear combination of these K basis codewords. The $K \times N$ matrix whose rows are the K basis codewords is called the generator matrix G of the code. G is of rank K . We note here that the elements of G are from $P_p^n[W(a)]$ which are themselves polynomials over $GF(p)$ and in variable a . If

$$u = (u_0 \ u_1 \ \dots \ u_{K-1}) \quad (5.2.1)^*$$

is the message word, corresponding codeword y is given by

$$y = u G \quad (5.2.2)^*$$

For a given G of rank K , there exists an $(N-K) \times N$ matrix H of rank $(N-K)$ such that $HG^{tr} = \underline{0}$. H is called the parity check matrix of the code C . If y is a codeword it is a linear combination of rows of G . Hence, $Hy^{tr} = \underline{0}$. On the other hand if any N -tuple y' is such that $Hy'^{tr} = \underline{0}$ then y'^{tr} is a linear combination of rows of G and hence is a codeword. Thus $Hy^{tr} = \underline{0}$ iff y is a codeword in C .

T

*In earlier chapters we have denoted n -tuples over $GF(p)$ as column vectors. However in this chapter we follow the standard practice in coding theory and write K -tuples and N -tuples over $P_p^n[W(a)]$ and n -tuples over $GF(p)$ as rows, denoted by lower case symbols.

If the code is such that any set of K fixed locations in the codewords have K message symbols, then the code is called a systematic code. For convenience in this section we assume that the first K symbols in the code are message symbols, i.e. $y_i = u_i$; $0 \leq i \leq (K-1)$, and the remaining $r = (N-K)$ symbols are the linear combination of message symbols called parity check symbols.

For a systematic (N,K) linear block code the $K \times N$ generator matrix is of the form

$$G = [I : P] \quad (5.2.3)$$

The corresponding $(N-K) \times K$ parity check matrix is

$$H = [-P^{tr} \quad I] \quad (5.2.4)$$

In (5.2.4) I is the $(N-K) \times (N-K)$ identity matrix and the $(N-K) \times K$ submatrix P^{tr} is transpose of P . The entries of P decide the linear relation between the message symbols and the parity check symbols.

In general the determination of K linearly independent N -tuples over $P_p^n[W(a)]$, which constitute the rows of G (of rank K) is difficult. However for a systematic code with G of the form (5.2.3), the K rows of G are necessarily linearly independent, and hence G is of rank K . The entries of $K \times (N-K)$ submatrix P which are from $P_p^n[W(a)]$ are chosen such that the code has specified error detecting/correcting capability.

The error detecting/correcting capability of the code depends on the minimum distance between codewords which we take up now.

5.2.1 Minimum Distance and Error Detecting/Correcting Capability

As in the case of linear block codes over finite fields the following is true for the linear block codes over $P_p^n[W(a)]$, where the weight structure is sufficient to know the minimum distance of the code.

Theorem 5.2.1 : In a linear block code over $P_p^n[W(a)]$, the minimum distance equals the minimum weight.

Proof : The linear structure of the code implies that given any two codewords y and z , their difference $(y-z)$ belongs to the code. Thus as seen in Section 4.4, the Hamming distance D_{yz} between y and z is equal to the Hamming weight $W_{(y-z)}$ of $y-z$.

$$\text{i.e.,} \quad D_{yz} = D_{y-z,0} = W_{y-z}$$

As a consequence the set of all distances between pairs of codewords of a linear code coincides with the set of all weights of its codewords.

*

In the case of block codes over a finite field if the minimum distance is d then $(d-1)$ errors can be detected or $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors can be corrected, where $\lfloor x \rfloor$ indicates largest

integer less than or equal to x . Codes can be used for error detection and/or error correction. For example all received N -tuples lying at a distance t or less from some codeword are decoded into that codeword, but if no codeword exists at such a distance from the received N -tuple, the latter is not decoded. In all N -tuples which contain at least $(t+1)$ but not more than $d-(t+1)$ channel errors, the error is detected. Therefore, if t or less errors are to be corrected and $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ then a t' number of errors can still be detected with $(t+1) \leq t' \leq (d-t-1)$. Hence a linear code can correct t errors and simultaneously detect t' errors iff $d \geq t' + t + 1$.

The above results are based on the additive abelian group structure of the code and the Hamming metric defined on that. Since a linear block code over $P_p^n[W(a)]$ also has the structure of an additive abelian group and the Hamming metric can be defined on this, the results hold here also.

Theorem 5.2.2 : If d is the minimum Hamming distance of a linear block code over $P_p^n[W(a)]$, then all sets of $\left\lfloor \frac{d-1}{2} \right\rfloor$ or less channel errors can be corrected.

Proof : Suppose the number of errors is $\leq \left\lfloor \frac{d-1}{2} \right\rfloor$. Then the received word is closer to the transmitted word in the Hamming distance sense. At least $\left\lfloor \frac{d-1}{2} \right\rfloor + 1$ errors are needed to make the received word closer to a codeword different from the transmitted one. Hence this code with minimum distance d is a $\left\lfloor \frac{d-1}{2} \right\rfloor$ error correcting code.

*

In a systematic (N, K) linear block code, K symbols correspond to the message word. A codeword can have atmost $(N-K)$ nonzero parity check symbols. A codeword with only one nonzero message symbol then can have weight atmost $(N-K+1)$. Hence the minimum distance d of a linear block code over $P_p^n[W(a)]$ satisfies the Singleton bound as given in [20].

$$d \leq (N-K+1) \quad (5.2.5)$$

Codes with $d = (N-K+1)$ are called maximum distance separable (MDS) codes. Reed Solomon codes [82] are the well known MDS codes over $GF(p^n)$ ($P_p^n[W(a)]$, where $W(a)$ is irreducible over $GF(p)$). Existence of codes analogous to Reed Solomon codes over residue class integer ring Z_m is investigated in [49].

The following lemma gives a bound on the length N of code-words in a code with a given minimum distance d .

Lemma 5.2.1 : In an (N, K) linear block code the necessary condition for the code to have minimum distance d is that N must be greater than or equal to d .

Proof : Using Singleton bound given in Expression (5.2.5), we have

$$d \leq N-K+1$$

i.e. $N \geq d+K-1$.

For a code K is at least one. Hence $N \geq d$. *

Corollary 5.2.1 : For a single error correcting linear block code, N is greater than or equal to 3.

Proof : The minimum distance of a single error correcting linear block code is 3. From the result of the above lemma $N \geq 3$. *

The inequality (5.1.2) is a necessary condition to be satisfied by any t error correcting code; it, however, does not guarantee the existence of a t error correcting code. For the existence of a t error correcting (N, K) linear block code, the parity check matrix H must satisfy certain conditions.

$$\text{Suppose } y = (y_0, y_1, \dots, y_{N-1}) \quad (5.2.6)$$

is the transmitted codeword and the error word is

$$e = (e_0, e_1, \dots, e_{N-1})$$

Then the received word is

$$y' = y + e$$

and

$$s(y') = Hy'^{\text{tr}} = H(y + e)^{\text{tr}} = He^{\text{tr}},$$

is called the syndrome of y' . If the columns of parity check matrix H are H_0, H_1, \dots, H_{N-1} then the syndrome can be written as

$$s(y') = e_0 H_0 + e_1 H_1 + \dots + e_{N-1} H_{N-1}$$

The parity check matrix H of a t error correcting (N,K) linear block code over $P_p^n[W(a)]$ must satisfy the following conditions.

1. For the detection of errors within the error detection capability of the code the syndromes should be nonzero for nonzero errors.

Suppose the error word is $(0,0,\dots, e_i, \dots, 0)$. The syndrome of y' is then $e_i H_i$. For the detection of the error e_i , the syndrome $e_i H_i$ should not be zero. Hence a necessary condition to be satisfied by the parity check matrix H is that none of its columns consists of only zeros, only zero divisors or a combination of zeros and zero divisors.

2. For the correction of t or less errors distinct error patterns should give rise to distinct syndromes. Any pattern of t or less errors will give rise to distinct syndrome if no linear combination of t or fewer columns of H equals another such linear combination. This puts a restriction on the columns of H that each set of $2t$ columns should be linearly independent. We prove this in the following theorem.

Theorem 5.2.3 : If the parity check matrix H of an (N,K) linear block code over $P_p^n[W(a)]$ is such that every set of $2t$ columns are linearly independent then any pattern of t or less errors will give rise to distinct syndrome.

Proof : Let e and e' be two distinct patterns of errors of weight t or less each. Then the syndromes are

$$He^{tr} = \sum_{i=0}^{N-1} e_i H_i \quad \text{and} \quad He'^{tr} = \sum_{i=0}^{N-1} e'_i H_i$$

where at most t of the coefficients e_i and e'_i respectively are nonzeros. Suppose the two syndromes are equal, then

$\sum_{i=0}^{N-1} (e_i - e'_i) H_i = \underline{0}$, where at most $2t$ coefficients $(e_i - e'_i)$ are nonzeros. This implies that linear combination of $2t$ or less columns of H is equal to column of zeros, i.e., $2t$ or less columns of H are linearly dependent. This contradicts the hypothesis that $2t$ columns of H are linearly independent. Hence, distinct patterns of errors of weight t or less give rise to distinct syndromes, if every set of $2t$ columns of H are linearly independent. *

Theorem 5.2.4 : If H is the parity check matrix of an (N, K) linear block code over $P_p^n[W(a)]$, then the code has minimum distance d , iff all sets of $(d-1)$ columns of H are linearly independent and some sets of d columns are linearly dependent.

Proof : Let the minimum distance of the code be d . Let

$z = (z_0 \ z_1 \ \dots, \ z_{N-1})$ be any nonzero N -tuple of weight less than d , i.e., at most $(d-1)$ z_i 's are nonzeros.

Hence z is necessarily not a codeword and $s(z) = Hz^{tr} = \sum_{i=0}^{N-1} z_i H_i \neq \underline{0}$. Thus linear combination of any set of $(d-1)$ or

less columns of H are linearly independent. Let

$y = (y_0, y_1, \dots, y_{N-1})$ be a codeword of weight d , then

$s(y) = Hy^{tr} = \sum_{i=0}^{N-1} y_i H_i = \underline{0}$, where d of the coefficients y_i are nonzeros. This implies that d columns of H are linearly dependent. Thus all sets of $(d-1)$ columns of H are linearly independent and some d columns are linearly dependent.

On the other hand suppose every set of $(d-1)$ columns of H is linearly independent and some sets of d columns of H are linearly dependent then, for N -tuples, $y' = (y'_0, y'_1, \dots, y'_{N-1})$ of weight $(d-1)$ or less only $(d-1)$ or less elements y'_i are non-zeros and $Hy'^{tr} = \sum_{i=0}^{N-1} y'_i H_i \neq \underline{0}$. This implies N -tuples of weight less than d are not codewords. Since some d columns of H are linearly dependent, there exists N -tuples y of weight d , such that $Hy^{tr} = \sum_{i=0}^{N-1} y_i H_i$ becomes zero. This implies that, N -tuples of weight greater than or equal to d are codewords. Hence the minimum distance is d . The foregoing results can be summarised as follows :

The minimum distance of a t error correcting (N, K) linear block code over $P_p^n[W(a)]$ should be at least equal to $(2t+1)$. If the minimum distance is equal to $(2t+1)$ every set of $2t$ columns of H must be linearly independent and some $(2t+1)$ columns are linearly dependent.

*

less columns of H are linearly independent. Let

$y = (y_0, y_1, \dots, y_{N-1})$ be a codeword of weight d , then

$s(y) = Hy^{tr} = \sum_{i=0}^{N-1} y_i H_i = \underline{0}$, where d of the coefficients y_i are nonzeros. This implies that d columns of H are linearly dependent. Thus all sets of $(d-1)$ columns of H are linearly independent and some d columns are linearly dependent.

On the other hand suppose every set of $(d-1)$ columns of H is linearly independent and some sets of d columns of H are linearly dependent then, for N -tuples, $y' = (y'_0, y'_1, \dots, y'_{N-1})$ of weight $(d-1)$ or less only $(d-1)$ or less elements y'_i are non-zeros and $Hy'^{tr} = \sum_{i=0}^{N-1} y'_i H_i \neq \underline{0}$. This implies N -tuples of weight less than d are not codewords. Since some d columns of H are linearly dependent, there exists N -tuples y of weight d , such that $Hy^{tr} = \sum_{i=0}^{N-1} y_i H_i$ becomes zero. This implies that, N -tuples of weight greater than or equal to d are codewords. Hence the minimum distance is d . The foregoing results can be summarised as follows :

The minimum distance of a t error correcting (N, K) linear block code over $P_p^n[W(n)]$ should be at least equal to $(2t+1)$. If the minimum distance is equal to $(2t+1)$ every set of $2t$ columns of H must be linearly independent and some $(2t+1)$ columns are linearly dependent.

The existence of a t error correcting (N,K) linear block code over $P_p^n[W(a)]$ depends on the existence of a matrix H with its elements from $P_p^n[W(a)]$, whose rank is $(N-K)$ and in which every set of $2t$ columns is linearly independent. It appears that existence of such matrices strongly depends on the number of units in $P_p^n[W(a)]$; an expression for the number of units in $P_p^n[W(a)]$ is given in Appendix F.

Example 5.2.2 : In this example we check the existence of a single error correcting $(5,3)$ linear block code over $P_2^2[a^2+1]$. The necessary condition for a $(5,3)$ linear block code over $P_2^2[a^2+1]$ with t error correcting capability to exist is given by Inequality (5.1.2).

Here $N = 5$, $K = 3$, $t = 1$, $p = 2$ and $q = 2^2 = 4$

we have $q^{(N-K)} = 2^{2(5-3)} = 16$

and $\sum_{i=0}^1 (4-1)^i \binom{5}{i} = 1+3.5 = 4.5$

The inequality is satisfied. Therefore, a single error correcting $(5,3)$ linear code over $P_2^2[a^2+1]$ may exist. Now we investigate whether it is possible to get a 2×5 parity check matrix in which every set of two columns is linearly independent. It can be verified that with the elements from $P_2^2[a^2+1] = \{0,1,a,(1+a)\}$ where $(1+a)$ is a zero divisor, it is not possible to obtain the required 2×5 H matrix. Hence a $(5,3)$ single error correcting linear block code over $P_2^2[a^2+1]$ is not possible. However, it is possible to have a $(5,3)$ single error detecting code.

Example 5.2.3 : In this example we investigate the existence of a linear block code over $P_2^2[a^2+a+1]$ which is a finite field of order 4. In this case as in Example 5.2.2 the Inequality (5.1.2) is satisfied. In addition it is possible to obtain the required 2×5 matrix. For example, in

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & a & 1+a & 0 & 1 \end{bmatrix}$$

all sets of two columns of H are linearly independent. But all sets of three columns are not linearly dependent. For example,

$$1 \cdot \begin{pmatrix} 1 \\ 1+a \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + (1+a) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{2; a^2+a+1}.$$

Since any set of two columns of H is linearly independent no 5-tuple y' of weight 2 will make $Hy'^t = \underline{0}$. Hence minimum weight of the code with H as parity check matrix is 3. The code with parity check matrix H given above can therefore correct single errors. This is an example of single error correcting nonbinary Hamming code over $GF(2^2)$.

*

Example 5.2.4 : We investigate the existence of a $(6,3)$ linear block code over $P_2^2[a^2+1]$. For single error correction we have $t = 1$ and the left hand side of Inequality (5.1.2) is equal to $1+3 \times 6 = 19$ and the right hand side is equal to $(2^2)^3 = 64$. The inequality is satisfied. Hence it may be possible to get a single error correcting $(6,3)$ code.

One possible H matrix is

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ a & 1 & 1 & 0 & 1 & 0 \\ 0 & a & 1 & 0 & 0 & 1 \end{bmatrix}$$

Every set of two columns of H is linearly independent, Hence the code has minimum distance 3 and can correct all patterns of single errors. On the other hand a (6,3) double error correcting code over $P_2^2[a^2+1]$ is not possible. This is because for $t = 2$ we have right hand side of Inequality (5.1.2) equal to 64 and left hand side equal to 139 and the inequality is not satisfied.

*

Example 5.2.5 : We investigate the existence of a (3,1) linear block code over $P_2^2[a^2+1]$. For single error correction, $t = 1$, the right hand side of Inequality (5.1.2) is

$$2^{2(3-1)} = 16$$

and the left hand side is 10.

The Inequality (5.1.2) is satisfied.

Hence it may be possible to get a single error correcting (3,1) code. One possible H matrix is

$$H = \begin{bmatrix} 1 & 1 & 0 \\ a & 0 & 1 \end{bmatrix}$$

Every set of two columns of H are linearly independent.
Hence $(3,1)$ single error correcting code over $P_2^2[a^2+1]$ exists.
However, since (5.1.2) is not satisfied with equality it is not a perfect code. *

We note in the above example that if the element a in the first column of H is replaced by 1, the $(3,1)$ linear block code becomes a repetition code and if the element a is replaced by the zero divisor $(1+a)$, the first two columns become linearly dependent. Then the minimum distance of the code is 2 and can only detect single errors.

Example 5.2.6: We investigate the existence of a $(5,3)$ linear block code over $P_2^2[a^2+a]$. For single error correction $t = 1$, the right hand side of inequality (5.1.2) is $2^{2(5-3)} = 16$ and the left hand side $1+3.5 = 16$.

The inequality is satisfied with equality.

Hence it may be possible to get a single error correcting $(5,3)$ code over $P_2^2[a^2+a]$.

One possible H matrix is

$$H = \begin{bmatrix} 1 & 1 & a & 1 & 0 \\ a & 1+a & 1+a & 0 & 1 \end{bmatrix}$$

Every set of two columns of H is not linearly independent.
Hence the minimum distance of the code is 2. Therefore, it can not correct single errors. However, it can detect single errors. *

Having discussed the factors which govern the choice of parity check matrix H of a linear block code over $P_p^n[W(a)]$, we now proceed to discuss the error detection and correction procedures for these codes.

5.2.2 Error Detection and Correction

The error detection/correction using an (N,K) linear block code C over $P_p^n[W(a)]$ is done by the calculation of syndrome of received words. In the previous section we have seen that the syndrome of any received word is zero iff it is a codeword. If the syndrome is nonzero an error is detected. The error correction is based on finding the coset corresponding to the syndrome and locating in it a minimum weight word which is the most likely error pattern. This error pattern is subtracted from the received word to get the transmitted word.

We next consider construction of cosets of C in the module V and a decoding procedure of linear block codes over $P_p^n[W(a)]$. The set V of all N -tuples over $P_p^n[W(a)]$ constitutes a module of rank N which is inherently an additive abelian group. C is a submodule of rank K and hence is a subgroup of V . We form cosets of C in V as indicated in Section 2.1. Two N -tuples V_1 and V_2 of V are in the same coset if

$$V_1 - V_2 \in C \quad (5.2.7)$$

Therefore,

$$H(V_1 - V_2)^{tr} = 0 \quad (5.2.8)$$

which implies,

$$HV_1^{tr} = HV_2^{tr} \quad (5.2.9)$$

The set of all N -tuples in the same coset have the same syndrome.

We show below that in an (N, K) block code over $P_p^n[W(a)]$ each coset corresponds to a distinct syndrome.

Theorem 5.2.5 : Each coset of linear block code C over $P_p^n[W(a)]$ corresponds to a distinct syndrome.

Proof : Let degree of $W(a)$ be n . Then order of $P_p^n[W(a)]$ is p^n . Number of possible N -tuples over $P_p^n[W(a)]$ is p^{nN} . Order of C is p^{nK} . Number of cosets is therefore $p^{n(N-K)}$. Syndrome is an $(N-K)$ -tuple over $P_p^n[W(a)]$. Hence the number of distinct syndromes is equal to $p^{n(N-K)}$.

If two N -tuples V_1 and V_2 have the same syndrome then from Equations (5.2.8) and (5.2.9), $(V_1 - V_2)$ is a codeword and hence V_1 and V_2 must be in the same coset. Therefore, each coset corresponds to a distinct syndrome.

*

We construct the cosets of C in the module of N -tuples over $P_p^n[W(a)]$. The N -tuple with minimum weight in each coset is chosen as the coset leader. If there are more than one minimum

weight N -tuples in a coset, any one of them is chosen as the leader. Each coset is associated with one of the $p^{n(N-K)}$ syndromes. The array of cosets of C in V is called standard array.

The error correcting capability of a linear code depends on the weights of the coset leaders, which are the correctable error patterns. A table which gives the set of syndromes and the associated coset leaders is called Decoding Table.

To correct all patterns of t errors, all patterns of words of weight t or less must have distinct syndromes. In other words all words of weight t or less should be in different cosets and they must be coset leaders. Once the syndrome is calculated the corresponding coset leader (it is the least weight word in the coset) is found and subtracted from the received word. If in the coset there are more than one member with the same least weight an error is detected, which cannot be corrected. However, in maximum likelihood decoding if there is a tie one of them is chosen. This may give rise to a decoding error. If the number of errors is more than the error correcting capability, the received word is different from the transmitted codeword but may still be another codeword. In this case the syndrome is zero and there is a decoding error. The decoding principle described above is similar to decoding of linear block codes over $GF(2)$ and is called syndrome decoding

(table look up decoding) [21]. Syndrome decoding can be applied to any (N,K) linear code. However, for large $(N-K)$, the implementation of this decoding scheme becomes impractical, as large storage is needed.

Example 5.2.7 : Consider a $(3,1)$ linear block code C over $P_2^2[a^2+1]$, with the parity check matrix $H = \begin{bmatrix} 1 & 1 & 0 \\ a & 0 & 1 \end{bmatrix}$ and generator matrix $G = [1 \ 1 \ a]$. We note that any two columns of H are linearly independent but not 3. Hence, minimum distance of code is 3 and the code can correct single errors and detect 2 errors.

The message words and the corresponding codewords over $P_2^2[a^2+1]$ and $Z_2^2 \cong P_2^2[a^2+1]$ are given in Table 5.2.2a. The cosets of C and the associated syndromes are given in Table 5.2.2b.

Number of possible 3-tuples over $P_2^2[a^2+1]$ is 64

Number of codewords is 4

Hence number of cosets is $64/4 = 16$.

*

In case of two errors the corresponding coset contains more than one 3-tuple with weight 2. Hence it is not possible to correct 2 errors.

Referring to the Table 5.2.2b suppose $y' = (1 \ a \ 1)$ is the received word then

$$Hy'^t = \begin{bmatrix} 1 & 1 & 0 \\ a & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ a \\ 1 \end{bmatrix} = \begin{bmatrix} 1+a \\ 1+a \end{bmatrix}.$$

Table 5.2.2a: Message and codewords of the (3,1) single error correcting code of Example 5.2.7.

$P_2^2[a^2+1]$		$Z_2^2 \cdot P_2^2[a^2+1]$	
Message words	Code words	Message words	Code words
0	(0 0 0)	(0 0)	(00 00 00)
1	(1 1 a)	(1 0)	(10 10 01)
a	(a a 1)	(0 1)	(01 01 10)
1+a	(1+a 1+a 1+a)	(1 1)	(11 11 10)

Table 5.2.2b: Cosets and associated syndromes of the (3,1) Linear block code C of Example 5.2.7.

Coset leaders	Cosets									Syndromes*	
0 0 0	1	1	a	a	a	1	1+a	1+a	1+a	0	0
0 0 1	1	1	1+a	a	a	0	1+a	1+a	a	0	1
0 0 a	1	1	0	a	a	1+a	1+a	1+a	1	0	a
0 0 1+a	1	1	1	a	a	a	1+a	1+a	0	0	1+a
0 1 0	1	0	a	a	1+a	1	1+a	a	1+a	1	0
0 a 0	1	1+a	a	a	0	1	1+a	1	1+a	a	0
0 1+a 0	1	a	a	a	1	1	1+a	0	1+a	1+a	0
1 0 0	0	1	a	1+a	a	1	a	1+a	1+a	1	a
a 0 0	1+a	1	a	0	a	1	1	1+a	1+a	a	1
1+a 0 0	a	1	a	1	a	1	0	1+a	1+a	1+a	1+a
0 1 1	1	0	1+a	a	1+a	0	1+a	a	a	1	1
0 1 1+a	1	0	1	a	1+a	a	1+a	a	0	1	1+a
0 a a	1	1+a	0	a	0	1+a	1+a	1	1	a	a
0 a 1+a	1	1+a	1	a	0	a	1+a	1	0	a	1+a
0 1+a 1	1	a	1+a	a	1	0	1+a	0	a	1+a	1
0 1+a a	1	a	0	a	1	1+a	1+a	0	1	1+a	a

*For the sake of convenience syndrome is written as a row 2-tuple.

The coset leader associated with this syndrome is $(1+a \ 0 \ 0)$. Subtracting the coset leader from the received word we get $(a \ a \ 1)$ which is the transmitted word.

On the other hand suppose $(a, 1, 1+a)$ is received. The syndrome is

$$\begin{bmatrix} 1 & 1 & 0 \\ a & 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ 1 \\ 1+a \end{bmatrix} = \begin{bmatrix} 1+a \\ a \end{bmatrix}.$$

In this case there are more than one minimum weight word in the coset; these are $(0 \ 1+a \ a)$, $(1 \ a \ 0)$ and $(1+a \ 0 \ 1)$. If the decoder is such that it chooses any one of these as in maximum likelihood decoder, a decoding error may result.

Example 5.2.8 : Consider the $(3,1)$ linear block code C over

$P_2^2[a^2+1]$ with $H = \begin{bmatrix} a & 1 & 0 \\ 1+a & 0 & 1 \end{bmatrix}$ and $G = [1 \ a \ 1+a]$. Since $(1+a) \begin{bmatrix} a \\ 1+a \end{bmatrix} + (1+a) \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ modulo $[2; a^2+1]$, the first and

and second columns are linearly dependent. The minimum distance is less than 3. However, all the columns are individually linearly independent, hence the minimum distance of the code is 2 and can only detect all patterns of single errors. The message words and the corresponding codewords over $P_2^2[a^2+1]$ and isomorphic Z_2^2 are given in Table 5.2.3a. The cosets and the associated syndromes are given in Table 5.2.3b.

Table 5.2.3a: Message and code words of the $(3,1)$ single error detecting code of Example 5.2.8.

$P_2^2[x^2+1]$		$L_2^2 \approx P_2^2[x^2+1]$	
Message word	code word	message word	Code word
0	(0 0 0)	00	(00 00 00)
1	(1 a 1+a)	10	(10 01 11)
a	(a 1 1+a)	01	(01 10 11)
1+a	(1+a 1+a 0)	11	(11 11 00)

Table 5.2.3b: Cosets and associated syndromes of $(3,1)$ linear block code C of Example 5.2.8.

Coset leader	Cosets									Syndrome*
0 0 0	1	a	1+a	a	1	1+a	1+a	1+a	0	0 0
0 0 1	1	a	a	a	1	a	1+a	1+a	1	0 1
0 0 a	1	a	1	a	1	1	1+a	1+a	a	0 a
0 0 1+a	1	a	0	a	1	0	1+a	1+a	1+a	0 1+a
0 1 0	1	1+a	1+a	a	0	1+a	1+a	a	0	1 0
0 a 0	1	0	1+a	a	1+a	1+a	1+a	1	0	a 0
0 1+a 0	1	1	1+a	a	a	1+a	1+a	0	0	1+a 0
1 0 0	0	a	1+a	1+a	1	1+a	a	1+a	0	a 1+a
a 0 0	1+a	a	1+a	0	1	1+a	1	1+a	0	1 1+a
0 1 1	1	1+a	a	a	0	a	1+a	a	1	1 1
0 a a	1	0	1	a	1+a	1	1+a	1	a	a a
0 1+a 1	1	1	a	a	a	a	1+a	0	1	1+a 1
0 1+a a	1	1	1	a	a	1	1+a	0	a	1+a a
0 1+a 1+a	1	1	0	a	a	0	1+a	0	1+a	1+a 1+a
0 1 a	1	1+a	1	a	0	1	1+a	a	a	1 a
0 a 1	1	0	a	a	1+a	a	1+a	1	1	a 1

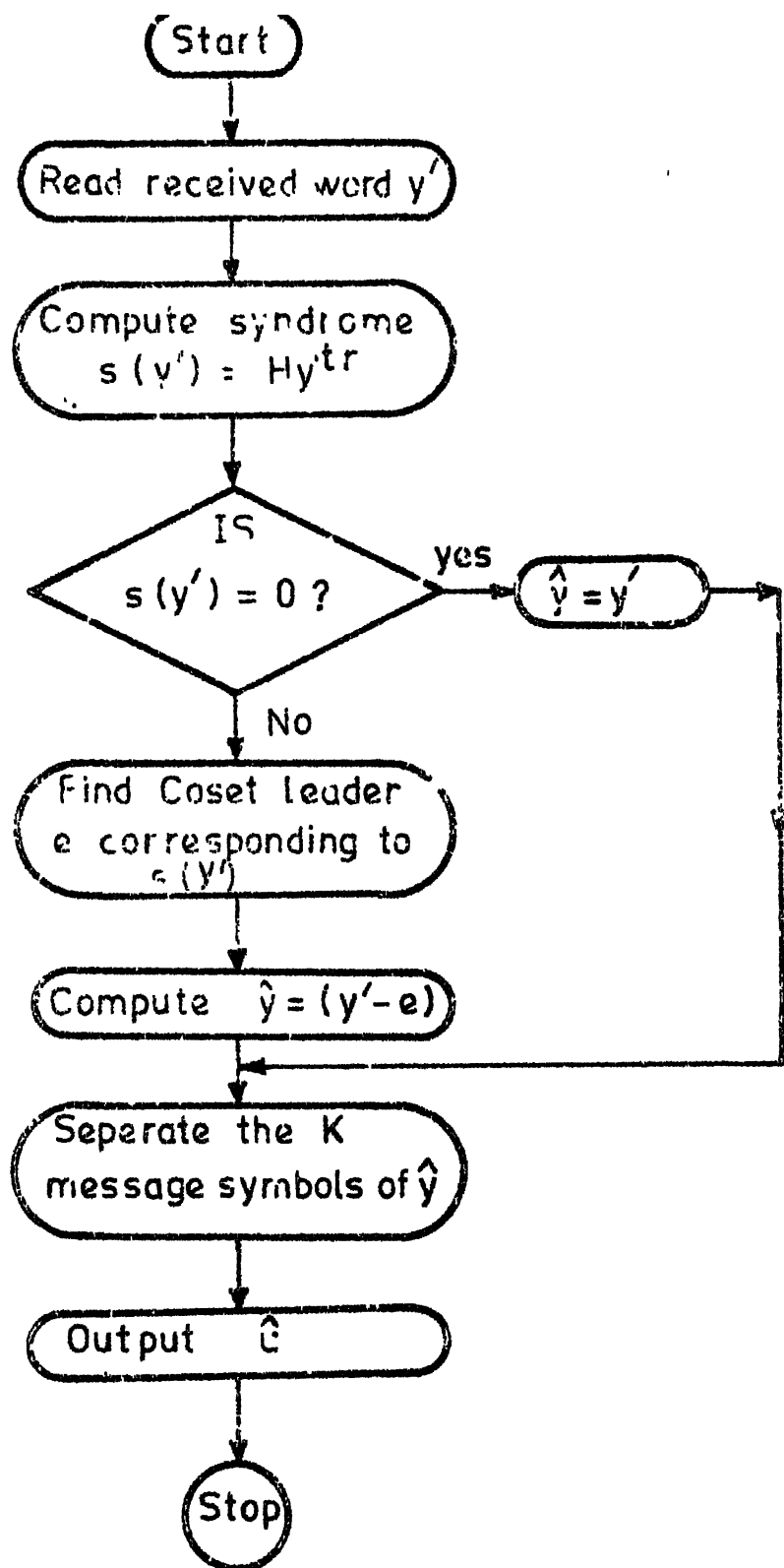
* For the sake of convenience syndrome is given as a row 2-tuple. We note here that the syndromes are distinct.

Referring to the Table 5.2.3b we note that,

- i) all patterns of single errors can be detected but all patterns of single errors cannot be corrected. However, all single error patterns except $(0 \ 1+a \ 0)$ and $(1+a \ 0 \ 0)$ can be corrected. This is because these two single error patterns are in the same coset and give rise to same syndrome. This implies that the errors at locations 1 and 2 of value $(1+a)$ cannot be distinguished.
- ii) none of the double errors can be corrected. This is because in each of the cosets whose coset leader has weight 2 we have another word of weight 2 having the same syndrome.
- iii) If the number of errors is three there is decoding error. For example if $(1 \ a \ 1+a)$ is the transmitted codeword and the received word is $(1+a \ 1+a \ 0)$ the syndrome is zero and the received word is decoded as $(1+a \ 1+a \ 0)$ resulting in decoding error.

*

Having discussed the construction of decoding table we now give the decoding procedure. This procedure is based on the fact that each coset corresponds to a distinct syndrome and uses the maximum likelihood or minimum distance criteria for decoding. When the messages are equiprobable this procedure is optimal and minimises the probability of error. The procedure is given in Flow Chart No. 5.2.1 and is similar to the syndrome decoding [21] for decoding linear block codes over $GF(2)$.



Flow Chart 5.21 Decoding Procedure for Linear Block Codes.

Example 5.2.9 : Consider the (3,1) linear block code C over $P_2^2[a^2+1]$ of Example 5.2.7. Suppose the received word is $y' = (a \ 1+a \ a)$. Referring to Table 5.2.2b, the syndrome is $S(y') = \begin{bmatrix} 1 \\ 1+a \end{bmatrix}$.

The corresponding coset leader is $(0 \ 1 \ 1+a)$.

Hence, the most likely transmitted word is

$$\begin{aligned} y &= y' - e \\ &= (a \ 1+a \ a) - (0 \ 1 \ 1+a) \\ &= (a \ a \ 1) \end{aligned}$$

which is the corrected word.

If the received codeword is considered to be over $Z_2^2 \simeq P_2^2[a^2+1]$ then $y' = (01 \ 11 \ 01)$, $S(y') = \begin{bmatrix} 10 \\ 11 \end{bmatrix}$ and the corresponding coset leader is $e = (00, 10, 11)$.

The most likely transmitted word is therefore,

$$\begin{aligned} y &= y' - e = (01 \ 11 \ 01) - (00 \ 10 \ 11) \\ &= (01 \ 01 \ 10) \end{aligned}$$

which is the corrected word.

5.3 LINEAR POLYNOMIAL CODES OVER $P_p^n[W(a)]$

In this section we study a class of (N,K) linear block codes over $P_p^n[W(a)]$ in which, codewords expressed as polynomials in x are multiples of an appropriately chosen fixed polynomial $g(x)$ of degree $r = (N-K)$. Such codes are called polynomial codes over $P_p^n[W(a)]$. It is shown that a polynomial code is the set of all zero state responses of a feed forward LSS with message words as inputs. Polynomial codes can thus be encoded by appropriate $P_p^n[W(a)]$ -LSS. Error detection is done by polynomial division. The remainder after the division operation is equal to the syndrome and a nonzero remainder indicates an error; correction is done by using decoding table as in the case of linear block codes discussed in the previous section.

5.3.1 Generating Polynomial, Generator Matrix and Encoding Principles

As pointed out above in polynomial code every codeword is a multiple of a fixed polynomial $g(x) = g_0 + g_1x + \dots + g_r x^r$ over $P_p^n[W(a)]$, called the generating polynomial of the code.

Let $\underline{u} = (u_0, u_1, \dots, u_{K-1})$ $u_i \in P_p^n[W(a)]$ be a message word. The set of all such K -tuples over $P_p^n[W(a)]$

$$\{\underline{u} = (u_0, u_1, \dots, u_{K-1}) \mid u_i \in P_p^n[W(a)]\} \quad (5.3.1)$$

constitutes a module which is free and is of rank K . The message word u can also be represented by a polynomial

$$u(x) = u_0 + u_1 x + u_2 x^2 + \dots + u_{K-1} x^{K-1} \quad (5.3.2)$$

called message polynomial. Note that the coefficients u_i themselves are polynomials over $GF(p)$ in the variable a . The set

$$\{u = u(x) \mid \text{degree } u(x) \leq (K-1), u_i \in P_p^n[W(a)]\} \quad (5.3.3)$$

constitutes a free module of rank K since it satisfies the following module axioms.

$$\alpha, \beta \in P_p^n[W(a)], u(x), u'(x) \in u$$

$$\alpha(u(x) + u'(x)) = \alpha u(x) + \alpha u'(x) = \sum_{i=0}^{K-1} (\alpha u_i + \alpha u'_i) x^i$$

$$(\alpha + \beta) u(x) = \alpha u(x) + \beta u(x) = \sum_{i=0}^{K-1} (\alpha u_i + \beta u_i) x^i$$

$$(\alpha\beta) u(x) = \alpha(\beta u(x))$$

$$\text{and } 1 \cdot u(x) = u(x)$$

The modules given by Expressions (5.3.1) and (5.3.3) are isomorphic to each other.

Consider the set of all formal power series over $P_p^n[W(a)]$, whose elements are of the form

$$z(x) = \sum_{i=0}^{\infty} z_i x^i$$

constitutes a module which is free and is of rank K . The message word u can also be represented by a polynomial

$$u(x) = u_0 + u_1 x + u_2 x^2 + \dots + u_{K-1} x^{K-1} \quad (5.3.2)$$

called message polynomial. Note that the coefficients u_i themselves are polynomials over $GF(p)$ in the variable a . The set

$$\{u = u(x) \mid \text{degree } u(x) \leq (K-1), u_i \in P_p^n[W(a)]\} \quad (5.3.3)$$

constitutes a free module of rank K since it satisfies the following module axioms.

$$\alpha, \beta \in P_p^n[W(a)], u(x), u'(x) \in u$$

$$\alpha(u(x) + u'(x)) = \alpha u(x) + \alpha u'(x) = \sum_{i=0}^{K-1} (\alpha u_i + \alpha u'_i) x^i$$

$$(\alpha + \beta) u(x) = \alpha u(x) + \beta u(x) = \sum_{i=0}^{K-1} (\alpha u_i + \beta u_i) x^i$$

$$(\alpha\beta) u(x) = \alpha(\beta u(x))$$

$$\text{and } 1 \cdot u(x) = u(x)$$

The modules given by Expressions (5.3.1) and (5.3.3) are isomorphic to each other.

Consider the set of all formal power series over $P_p^n[W(a)]$, whose elements are of the form

$$z(x) = \sum_{i=0}^{\infty} z_i x^i$$

This set constitutes a commutative ring denoted by $P_p^n[W(a)][x]$. This ring can also be regarded as a $P_p^n[W(a)]$ -module.

Consider the two polynomials : $u(x) = u_0 + u_1x + \dots + u_{K-1}x^{K-1}$ and $g(x) = g_0 + g_1x + \dots + g_r x^r$ over $P_p^n[W(a)][x]$.

For a given $g(x)$ the set C of all polynomials

$$\{y(x) = u(x) \cdot g(x) \mid u(x) \text{ of degree } \leq K-1\}$$

constitutes a free submodule of rank K . C constitutes a linear block code if $g(x)$ is such that i) the order of the submodule C is p^{nK} and ii) given $y(x) = u(x) \cdot g(x)$ it is possible to get back $u(x)$. These conditions may not be satisfied by an arbitrarily selected $g(x)$. Hence for $g(x)$ to be a generator polynomial it should satisfy certain constraints on its coefficients. Towards obtaining these constraints consider the following example.

Example 5.3.1 :

Consider the 16 message words given by message polynomials of degree atmost equal to one over $P_2^2[a^2+1]$. The corresponding polynomial products $y(x) = u(x) \cdot g(x)$ for the following cases are considered.

- (i) $g(x) = (1+a) + (1+a)x + (1+a)x^2$; all the coefficients are zero divisors
- (ii) $g(x) = (1+a) + ax + (1+a)x^2$; coefficient g_1 is a unit
- (iii) $g(x) = a + (1+a)x + (1+a)x^2$; coefficient g_0 is a unit
- (iv) $g(x) = (1+a) + (1+a)x + ax^2$; coefficient g_2 is a unit .

The polynomial products for the cases (i) and (ii) are listed in Table 5.3.1a and the products for the cases (iii) and (iv) are listed in Table 5.3.1b. The corresponding 4 tuples over $\mathbb{Z}_2^2 \cong \mathbb{P}_2^2[a^2+1]$ are given in Tables 5.3.2a and 5.3.2b respectively.

We observe that in case (i) more than one $u(x)$ results in the same $y(x)$. The other three cases give rise to a unique $y(x)$ for a given $u(x)$. Hence to have a unique $y(x)$ for a given $u(x)$, the necessary condition is that all the coefficients of $g(x)$ should not be zero divisors in $\mathbb{P}_p^n[W(a)]$. However, if g_0 and g_2 are both zero divisors but g_1 is a unit as in case (ii), given $y(x)$, $u(x)$ cannot be determined by dividing $y(x)$ by $g(x)$. For example suppose $y(x) = (1+a)+x+ax^2+(1+a)x^3$ is given. We perform long division of $y(x)$ by $g(x)$ and see that the remainder is not zero and the quotient is not the corresponding $u(x) = 1+ax$.

If either g_0 or g_2 is a unit as in cases (iii) and (iv) given $y(x)$, $u(x)$ can be determined by long division. For example consider case (iii).

Let $y(x) = (1+a)+ax+(1+a)x^2+(1+a)x^3$; dividing $y(x)$ by $g(x) = a+(1+a)x+(1+a)x^2$, (g_0 is a unit), we get zero remainder and quotient is the corresponding $u(x) = (1+a)+x$.

Table 5.3.1a $u(x)$ and $y(x) = u(x) \cdot g(x)$ of Example 5.3.1

$u(x)$	$y(x) = u(x) \cdot g(x);$ (i) $g(x) = (1+a) + (1+a)x + (1+a)x^2$	$y(x) = u(x) \cdot g(x);$ (ii) $g(x) = (1+a) + ax + (1+a)x^2$
0	0	0
1	$(1+a) + (1+a)x + (1+a)x^2$	$(1+a) + ax + (1+a)x^2$
a	$(1+a) + (1+a)x + (1+a)x^2$	$(1+a) + x + (1+a)x^2$
$(1+a)$	0	$(1+a)x$
x	$(1+a)x + (1+a)x^2 + (1+a)x^3$	$(1+a)x + ax^2 + (1+a)x^3$
ax	$(1+a)x + (1+a)x^2 + (1+a)x^3$	$(1+a)x + x^2 + (1+a)x^3$
$(1+a)x$	0	$(1+a)x^2$
$(1+x)$	$(1+a) + (1+a)x^3$	$(1+a) + x + x^2 + (1+a)x^3$
$(a+x)$	$(1+a) + (1+a)x^3$	$(1+a) + ax + x^2 + (1+a)x^3$
$(1+a) + x$	$(1+a)x + (1+a)x^2 + (1+a)x^3$	$ax^2 + (1+a)x^3$
$1+ax$	$(1+a) + (1+a)x^3$	$(1+a) + x + ax^2 + (1+a)x^3$
$a+ax$	$(1+a) + (1+a)x^3$	$(1+a) + ax + ax^2 + (1+a)x^3$
$(1+a) + ax$	$(1+a)x + (1+a)x^2 + (1+a)x^3$	$x^2 + (1+a)x^3$
$1 + (1+a)x$	$(1+a) + (1+a)x + (1+a)x^2$	$(1+a) + ax$
$a + (1+a)x$	$(1+a) + (1+a)x + (1+a)x^2$	$(1+a) + x$
$\begin{Bmatrix} 1+a \\ 1+a \end{Bmatrix} x$	0	$(1+a)x + (1+a)x^2$

Table 5.3.1b: $u(x)$ and $y(x) = u(x) \cdot g(x)$ of Example 5.3.1.

$u(x)$	i) $y(x)=u(x) \cdot g(x);$	ii) $y(x)=u(x) \cdot g(x);$
	iii) $g(x)=a+(1+a)x+(1+a)x^2$	iv) $g(x)=(1+a)+(1+a)x+ax^2$
0	0	0
1	$a+(1+a)x+(1+a)x^2$	$(1+a)+(1+a)x+ax^2$
a	$1+(1+a)x+(1+a)x^2$	$(1+a)+(1+a)x+x^2$
$(1+a)$	$(1+a)$	$(1+a)x^2$
x	$ax+(1+a)x^2+(1+a)x^3$	$(1+a)x+(1+a)x^2+ax^3$
ax	$x+(1+a)x^2+(1+a)x^3$	$(1+a)x+(1+a)x^2+x^3$
$(1+a)x$	$(1+a)x$	$(1+a)x^3$
$(1+x)$	$a+x+(1+a)x^3$	$(1+a)+x^2+ax^3$
$(a+x)$	$1+x+(1+a)x^3$	$(1+a)+ax^2+ax^3$
$(1+a)+x$	$(1+a)+ax+(1+a)x^2+(1+a)x^3$	$(1+a)x+ax^3$
$1+ax$	$a+ax+(1+a)x^3$	$(1+a)+x^2+x^3$
$a+ax$	$1+ax+(1+a)x^3$	$(1+a)+ax^2+x^3$
$(1+a)+ax$	$(1+a)+x+(1+a)x^2+(1+a)x^3$	$(1+a)x+x^3$
$1+(1+a)x$	$a+(1+a)x^2$	$(1+a)+(1+a)x+ax^2+(1+a)x^3$
$a+(1+a)x$	$1+(1+a)x^2$	$(1+a)+(1+a)x+x^2+(1+a)x^3$
$(1+a)+(1+a)x$	$(1+a)+(1+a)x$	$(1+a)x^2+(1+a)x^3$

Table 5.3.2a: u and y of Example 5.3.1

		i) $g(x)=(1+a)+(1+a)x+(1+a)x^2$	ii) $g(x)=(1+a)+ax+(1+a)x^2$
\underline{u}	y	y	
(00 00)	(00 00 00 00)	(00 00 00 00)	
(10 00)	(11 11 11 00)	(11 01 11 00)	
(01 00)	(11 11 11 00)	(11 10 11 00)	
(11 00)	(00 00 00 00)	(00 11 00 00)	
(00 10)	(00 11 11 11)	(00 11 01 11)	
(00 01)	(00 11 11 11)	(00 11 10 11)	
(00 11)	(00 00 00 00)	(00 00 11 00)	
(10 10)	(11 00 00 11)	(11 10 10 11)	
(11 10)	(00 11 11 11)	(00 00 01 11)	
(10 01)	(11 00 00 11)	(11 10 01 11)	
(01 01)	(11 00 00 11)	(11 01 01 11)	
(11 01)	(00 11 11 11)	(00 00 10 11)	
(10 11)	(11 11 11 00)	(11 01 00 00)	
(01 11)	(11 11 11 00)	(11 10 00 00)	
(11 11)	(00 00 00 00)	(00 11 11 00)	
(01 10)	(11 00 00 11)	(11 01 10 11)	

Table 5.3.2b: \underline{u} and \underline{y} of Example 5.3.1

iii) $g(x)=a+(1+a)x+(1+a)x^2$					iv) $g(x)=(1+a)+(1+a)x+ax^2$			
<u>u</u>	<u>y</u>				<u>y</u>			
(00 00)	(00	00	00	00)	(00	00	00	00)
(10 00)	(01	11	11	00)	(11	11	01	00)
(01 00)	(10	11	11	00)	(11	11	10	00)
(00 10)	(00	01	11	11)	(00	11	11	01)
(00 01)	(00	10	11	11)	(00	11	11	10)
(00 11)	(00	11	00	00)	(00	00	00	11)
(10 10)	(01	10	00	11)	(11	00	10	01)
(01 10)	(10	10	00	11)	(11	00	01	01)
(11 10)	(11	01	11	11)	(00	11	00	01)
(10 01)	(01	01	00	11)	(11	00	10	10)
(01 01)	(10	01	00	11)	(11	00	01	10)
(11 01)	(11	10	11	11)	(00	11	00	10)
(10 11)	(01	00	11	00)	(11	11	01	11)
(01 11)	(10	00	11	00)	(11	11	10	11)
(11 11)	(11	11	00	00)	(00	00	11	11)
(11 00)	(11	00	00	00)	(00	00	11	00)

Consider Case (iv)

Let $y(x) = (1+a) + (1+a)x + x^2 + (1+a)x^3$; dividing $y(x)$ by $g(x) = (1+a) + (1+a)x + ax^2$ (g_2 is a unit) we get zero remainder and quotient is the corresponding $u(x) = a + (1+a)x$.

Now we show that in order to obtain $u(x)$ uniquely from $y(x)$ by long division the generator polynomial should satisfy the condition given by the theorem below :

Theorem 5.3.1 : A one-to-one correspondence between $u(x)$ and $y(x)$ is established iff either the coefficient g_0 or g_r of the generating polynomial $g(x)$ is a unit in $P_p^n[W(a)]$.

Proof : Suppose g_0 is a unit in $P_p^n[W(a)]$, then g_0^{-1} is defined. Given $u(x) = u_0 + u_1x + \dots + u_{K-1}x^{K-1}$ the coefficients of $y(x) = y_0 + y_1x + \dots + y_{N-1}x^{N-1}$ are uniquely determined by the following relation :

$$y_i = \sum_{j=0}^i g_j u_{i-j} ; i = 0, 1, \dots, N-1 ; u_{i-j} = 0 \text{ for } 0 < i-j < (K-1) \quad (5.3.4)$$

For a given $y(x)$ then coefficients of $u(x)$ can be determined uniquely by the following relations.

From the relation (5.3.4) we have,

$$y_0 = g_0 u_0, \text{ therefore, } u_0 = g_0^{-1} y_0$$

$$y_1 = g_0 u_1 + g_1 u_0 ; \text{ therefore, } u_1 = g_0^{-1} (y_1 - g_1 u_0) = g_0^{-1} (y_1 - g_1 g_0^{-1} y_0)$$

$$y_2 = g_0 u_2 + g_1 u_1 + g_2 u_0 ;$$

$$\text{therefore } u_2 = g_0^{-1}(y_2 - g_1 u_1 - g_2 u_0) = g_0^{-1}(y_2 - g_1 g_0^{-1}(y_1 - g_1 g_0^{-1} y_0) - g_2 g_0^{-1} y_0) .$$

$$y_3 = g_0 u_3 + g_1 u_2 + g_2 u_1 + g_3 u_0 ,$$

$$\begin{aligned} \text{therefore, } u_3 &= g_0^{-1}(y_3 - g_1 u_2 - g_2 u_1 - g_3 u_0) \\ &= g_0^{-1}(y_3 - g_1 g_0^{-1}(y_2 - g_1 g_0^{-1}(y_1 - g_1 g_0^{-1} y_0) - g_2 g_0^{-1} y_0) - g_2 g_0^{-1}(y_1 - g_1 g_0^{-1} y_0) - g_3 g_0^{-1} y_0) . \end{aligned}$$

In general given $y(x)$, u_i can be expressed in terms of $u_{i-1}, u_{i-2}, \dots, u_1, u_0$ and y_i by the recursive relation

$$u_0 = g_0^{-1} y_0$$

and

$$u_i = g_0^{-1} [y_i - \sum_{j=1}^i g_j u_{i-j}] \dots 0 < i \leq (K-1) \quad (5.3.5)$$

Likewise if g_r is a unit then given $u(x)$ the coefficients of $y(x)$ are uniquely determined by the Relation (5.3.4). For a given $y(x)$ then coefficients of $u(x)$ can be determined uniquely by the following relations.

From the Relation (5.3.4) we have,

$$y_{N-1} = g_r u_{K-1}, \text{ therefore } u_{K-1} = g_r^{-1} y_{N-1}$$

$$\begin{aligned} y_{N-2} &= g_r u_{K-2} + g_{r-1} u_{K-1}, \text{ therefore } u_{K-2} = g_r^{-1}(y_{N-2} - g_{r-1} u_{K-1}) \\ &= g_r^{-1}(y_{N-2} - g_{r-1} g_r^{-1} y_{N-1}) \end{aligned}$$

$$y_{N-3} = g_r u_{K-3} + g_{r-1} u_{K-2} + g_{r-2} u_{K-1} ,$$

therefore,

$$\begin{aligned} u_{K-3} &= g_r^{-1}(y_{N-3}-g_{r-1}u_{K-2}-g_{r-2}u_{K-1}) \\ &= g_r^{-1}(y_{N-3}-g_{r-1}g_r^{-1}(y_{N-2}-g_{r-1}g_r^{-1}y_{N-1})-g_{r-2}g_r^{-1}y_{N-1}). \end{aligned}$$

In general u_{K-i} can be expressed in terms of $u_{K-1}, u_{K-2}, \dots, u_{K-i+1}$ and y_{N-i} by the recursive relation

$$u_{K-i} = g_r^{-1}[y_{N-i} - \sum_{j=1}^{i-1} g_{r-j}u_{K-i+j}] ; i = 2, 3, \dots, K \quad (5.3.6)$$

The first part of the theorem, that when either g_0 or g_r is a unit in $P_p^n[W(a)]$, there is one-to-one correspondence between $y(x)$ and $u(x)$, is thus established.

If there is a one-to-one correspondence between $y(x)$ and $u(x)$, then the coefficients of $u(x)$ and $y(x)$ must necessarily be related either as given by Relation (5.3.5) or (5.3.6), which imply that either g_0 or g_r is a unit in $P_p^n[W(a)]$. *

Example 5.3.2 : Consider the set of $u(x)$ and the polynomial products $u(x).g(x)$ over $P_2^2[a^2+1]$ given in Example 5.3.1 for cases

(iii) with $g(x) = a+(1+a)x+(1+a)x^2$, where g_0 is a unit and

(iv) with $g(x) = (1+a)+(1+a)x+ax^2$, where g_2 is a unit.

In these cases $u(x)$ is of degree less than or equal to one, $g(x)$ is of degree 2 and $y(x)$ is of degree less than or equal to 3. Given $u(x)$ the computation of $y(x)$ is the usual polynomial

multiplication which results in a unique $y(x)$. Given $y(x)$ the coefficients of $u(x)$ are determined by the following relations.

Case (iii) : Let $y(x) = (1+a)+ax+(1+a)x^2+(1+a)x^3$, using Relation (5.3.5),

$$u_0 = g_0^{-1}y_0 = a(1+a) = (1+a)$$

$$u_1 = g_0^{-1}(y_1 - g_1u_0) = a(a - (1+a) \cdot (1+a)) = a \cdot a = 1$$

$$u(x) = (1+a)+x.$$

Referring to Table 5.3.1b we note that $u(x)$ is indeed $(1+a)+x$. Likewise in case (iv)

let $y(x) = (1+a)+ax^2+ax^3$, using Relation (5.3.6)

$$u_1 = g_2^{-1}y_3 = a \cdot a = 1$$

$$u_0 = g_2^{-1}(y_2 - g_1u_1) = a(a - 1+a) = a$$

Therefore, $u(x) = a + x$.

Referring to Table 5.3.1b we note that $u(x)$ is indeed $a+x$.

Theorem 5.3.2 : Let $g(x)$ be a polynomial of degree $r = N-K$ over $P_p^n[W(a)]$, with either g_0 or g_r a unit. Then the set

$$C = \{y(x) = u(x) \cdot g(x) \mid u(x) \text{ of degree } < K \text{ over } P_p^n[W(a)]\} \quad (5.3.7)$$

constitutes a submodule of rank K and order p^{nK} ,

$1, x, \dots, x^{K-1}$ is a basis* for this submodule. The set C hence constitutes an (N, K) linear block code over $P_p^n[W(a)]$.

Proof : We first prove that C is a module whose order is p^{nK} . Then show that it is a free module of rank K and hence is an (N, K) linear block code.

Let $y(x) = u(x) \cdot g(x)$ and $z(x) = v(x) \cdot g(x)$ be elements of C . Let α, β and $1 \in P_p^n[W(a)]$, where 1 is the identity element of C satisfies the following module axioms.

$$\alpha(y(x) + z(x)) = \alpha y(x) + \alpha z(x)$$

$$(\alpha + \beta) y(x) = \alpha y(x) + \beta y(x)$$

$$(\alpha \beta) y(x) = \alpha(\beta y(x))$$

$$\text{and } 1y(x) = y(x).$$

Therefore C is a $P_p^n[W(a)]$ -module.

Since either g_0 or g_r is a unit in $P_p^n[W(a)]$, each $u(x)$ gives rise to a distinct $y(x)$. Since there are p^{nK} polynomials of degree less than K over $P_p^n[W(a)]$, order of C is p^{nK} .

* Another useful basis for codes over finite fields which is not suitable here because of the presence of zero divisors, is given in Appendix G.

An arbitrary polynomial of degree less than K over $P_p^n[W(a)]$ can be expressed as a linear combination of $1, x, x^2, \dots, x^{K-1}$. Hence any element of C can be expressed as a linear combination of $g(x), xg(x), \dots, x^{K-1}g(x)$. Therefore, C is finitely generated and is of rank K .

C is a free module over $P_p^n[W(a)]$ whose order is p^{nK} and rank K . Hence C constitutes an (N, K) linear block code over $P_p^n[W(a)]$. Every codeword polynomial is a multiple of $g(x)$. Hence C is an (N, K) polynomial code over $P_p^n[W(a)]$, generated by $g(x)$.

*

Theorem 5.3.3 : A polynomial of degree less than N is a codeword polynomial of an (N, K) polynomial code over $P_p^n[W(a)]$ generated by $g(x)$ iff it is a multiple of $g(x)$ of degree $(N-K)$ with either g_o or g_r a unit.

Proof : Let $v(x)$ of degree less than N be a codeword polynomial generated by $g(x)$, over $P_p^n[W(a)]$. Since in polynomial code every codeword polynomial is a multiple of $g(x)$, $v(x)$ is a multiple of $g(x)$.

Suppose $v(x)$ of degree less than N over $P_p^n[W(a)]$ is a multiple of $g(x)$, then $v(x) = g(x) \cdot u'(x)$. Since either g_o or g_r a unit in $P_p^n[W(a)]$, the K coefficients u_0, u_1, \dots, u_{K-1} of $u'(x)$ can be uniquely determined using, the Recursion Relation (5.3.5) or (5.3.6) respectively. Then $v(x)$ is the codeword polynomial corresponding to message polynomial $u'(x)$ of degree less than K .

Generator Matrix : Since polynomial code is a linear block code any set of K linearly independent codewords constitutes the rows of Generator matrix G . It can be shown that if g_0 or g_r is a unit, then $g(x)$, $xg(x)$, ..., $x^{K-1}g(x)$ are linearly independent. Hence codewords corresponding to these K polynomials can be chosen as the K rows of G . Then the $K \times N$ generator matrix G given below has $(g_0, g_1, \dots, g_r, 0, \dots, 0)$ as the first row and the succeeding rows are the cyclic shifts of the preceding rows.

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ 0 & g_0 & g_1 & & g_r & \dots & 0 \\ \vdots & & & & & & \\ 0 & 0 & & g_0 & g_1 & \dots & g_r \end{bmatrix} \quad (5.3.8)$$

If $u = (u_0, u_1, \dots, u_{K-1})$ is the message word then $y = uG = (y_0, y_1, \dots, y_{N-2})$ is the codeword whose components

$$y_i = \sum_{j=0}^i u_j g_{i-j} \quad ; \quad i = 0, \dots, (N-1) \quad (5.3.9)$$

are the coefficients of x^i in the polynomial $y(x) = g(x) u(x)$.

The generator matrix G can also be written as

$$G = \begin{bmatrix} g_r & g_{r-1} & \dots & \dots & g_1 & g_0 & 0 & \dots & 0 \\ 0 & g_r & g_{r-1} & g_{r-1} & & g_1 & g_0 & \dots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & & & & g_r & g_{r-1} & & g_1 & g_0 \end{bmatrix} \quad (5.3.10)$$

However, in this case the message word is represented as

$$u = (u_{K-1} \ u_{K-2} \ \dots \ u_1 \ u_0)$$

and

$$y = uG = (y_{N-1} \ y_{N-2} \ \dots \ y_1 \ y_0)$$

where y_1 is given by the Relation (5.3.9).

We will see in Section 5.5 that the two representations (5.3.8) and (5.3.10) of the generator matrix give rise to two encoder structures.

It may be noted that the generator matrices given above by (5.3.8) and (5.3.10) are not in systematic form. However, because of restriction on the coefficients of $g(x)$ i.e., g_0 or g_r a unit in $P_p^n[W(a)]$, the rank of these matrices is K and a one to one correspondence between $u(x)$ and $g(x)$ is ensured. We note here that if g_r is a unit and g_0 is a zero divisor, even if u_0 is not zero, the constant term y_0 , in some code-word polynomials will be zero. Likewise if g_0 is a unit and

g_r a zero divisor, the least degree polynomial in the set of all codeword polynomials will have a degree less than r . Such a situation does not arise in the case of polynomial codes over $GF(p^n)$, in which all the nonzero field elements are units.

Example 5.3.3 : Consider $(3,1)$ polynomial codes generated by $g(x) = a+x+ax^2$ and $g(x) = a+(1+a)x+(1+a)x^2$ over $P_2^2[a^2+1]$.

Message words and the corresponding codewords over $P_2^2[a^2+1]$ and Z_2^2 are listed in Table 5.3.3. In the first case the least degree polynomial in the set of codeword polynomials is 2 and the minimum weight is 3. In the second case the least degree polynomial in the set of codeword polynomials is zero and the minimum weight is 1.

*

Encoding Principles : Encoding of an (N,K) polynomial code is based on the fact that every codeword in the code is the product of a generating polynomial $g(x)$ of degree $r = (N-K)$ and the message polynomial $u(x)$ of degree $\leq (K-1)$. A feed forward LSS whose impulse response is the first row of the generator matrix G or equivalently the set of coefficients of $g(x)$, will perform the multiplication of polynomials $u(x)$ and $g(x)$. As pointed out earlier, the generator matrix can be represented in two ways, as given by (5.3.8) and (5.3.10). Hence two implementations are possible. In the first case the codeword is represented by $y = (y_0 \ y_1 \ \dots \ y_{N-1})$ and in the second case the codeword is represented by $y = (y_{N-1} \ y_{N-2} \ \dots \ y_1 \ y_0)$

Table 5.3.3: Code word polynomials of (3,1) linear polynomial code of Example 5.3.3.

$g(x)=a+x+ax^2$		$g(x)=a+(1+a)x+(1+a)x^2$	
$u(x)$ over $P_2^2[a^2+1]$	\underline{u} over Z_2^2	$y(x)$ over $P_2^2[a^2+1]$	\underline{y} over Z_2^2
0	00	0	(00 00 00)
1	10	$a+x+ax^2$	(01 10 01)
a	01	$1+ax+x^2$	(10 01 10)
$1+a$	11	$(1+a)+$ $(1+a)x+$ $(1+a)x^2$	(11 11 11)

where y_i is the coefficient of x^i . In both cases the codeword polynomial is a multiple of $g(x)$; however, the code is not systematic.

Systematic (N,K) Polynomial Codes: For a specified $g(x)$, systematic polynomial code can be obtained by computing the parity check symbols in an appropriate $P_p^n[W(a)]$ -LSS, by polynomial division. The encoding operation depends on whether g_0 or g_r is a unit in $P_p^n[W(a)]$. This results in the following cases.

Case i) g_r a unit in $P_p^n[W(a)]$. This case is same as encoding systematic cyclic codes over finite fields [18-21]. The message word is denoted by

$u = (u_{K-1} \ u_{K-2} \ \dots \ u_1 u_0)$. The message word polynomial

$u(x) = u_{K-1}x^{K-1} + u_{K-2}x^{K-2} + \dots + u_1x + u_0$, is to be encoded into an (N,K) polynomial code. The codeword polynomial

$y(x) = y_{N-1}x^{N-1} + y_{N-2}x^{N-2} + \dots + y_1x + y_0$ then must be a multiple of

$g(x) = g_rx^r + g_{r-1}x^{r-1} + \dots + g_1x + g_0$. The encoding principle is as follows. $u(x)$ is multiplied, by x^{N-K} to get $u'(x) = x^{N-K}u(x)$.

$u'(x)$ is divided by $g(x)$ using $P_p^n[W(a)]$ -LSS of order r to get a quotient $q(x)$ and remainder $R(x)$. Degree of $R(x)$ is less than r and is of the form $R_{r-1}x^{r-1} + R_{r-2}x^{r-2} + \dots + R_1x + R_0$.

Hence $x^{N-K} u(x) = u'(x) = g(x) \cdot q(x) + R(x)$

or

$$u'(x) - R(x) = g(x) \cdot q(x)$$

Degree of $u'(x)$ is greater than $(r-1)$ and less than or equal to $N-1$. Hence, the symbols u_i and R_i are separated.

Setting $y_{r+i} = u_i \quad i = 0, 1, \dots, K-1,$

and $y_i = -R_i \quad i = 0, 1, \dots, r-1,$

$y(x) = u'(x) - R(x) = g(x) \cdot q(x)$ is a multiple of $g(x)$ and a valid codeword polynomial. The first K higher degree symbols are the message symbols.

Example 5.3.4

We consider an example of $(4,2)$ systematic polynomial code over $P_2^2[a^2+1]$ generated by $g(x) = ax^2 + (1+a)x + a$. The message word $u(x)$, polynomial $x^2 \cdot u(x)$, remainder $R(x)$ after dividing $x^2 \cdot u(x)$ by $g(x)$, and codeword polynomial $y(x) = x^2 \cdot u(x) - R(x)$ are given in Table 5.3.4a. The corresponding message u and codeword y over $Z_2^2 \simeq P_2^2[a^2+1]$ are also given in Table 5.3.4b.

All the codeword polynomials are multiples of $g(x)$. The codewords corresponding to message polynomials x and 1 can be taken as a basis. Then the matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 1+a \\ 0 & 1 & a+1 & 1 \end{bmatrix}$$

Table 5.3.4a Message and codeword polynomials of the (4,2) systematic polynomial code of Example 5.3.4

$P_2[a^2+1]$			
$u(x)$	$x^2 u(x)$	$R(x)$	$y(x)$
0	0	0	0
1	x^2	$(1+a)x+1$	$x^2+(1+a)x+1$
a	ax^2	$(1+a)x+a$	$ax^2+(1+a)x+a$
$(1+a)$	$(1+a)x^2$	$(1+a)$	$(1+a)x^2+(1+a)$
x	x^3	$x+(1+a)$	$x^3+x+(1+a)$
ax	ax^3	$ax+(1+a)$	$ax^3+ax+(1+a)$
$(1+a)x$	$(1+a)x^3$	$(1+a)x$	$(1+a)x^3+(1+a)x$
$x+1$	x^3+x^2	$ax+a$	x^3+x^2+ax+a
$x+a$	x^3+ax^2	$ax+1$	x^3+ax^2+ax+1
$x+(1+a)$	$x^3+(1+a)x^2$	x	$x^3+(1+a)x^2+x$
$ax+1$	ax^3+x^2	$x+a$	ax^3+x^2+x+a
$ax+a$	ax^3+ax^2	$x+1$	ax^3+ax^2+x+1
$ax+(1+a)$	$ax^3+(1+a)x^2$	ax	$ax^3+(1+a)x^2+ax$
$(1+a)x+1$	$(1+a)x^3+x^2$	1	$(1+a)x^3+x^2+1$
$(1+a)x+a$	$(1+a)x^3+ax^2$	a	$(1+a)x^3+ax^2+a$
$(1+a)x+(1+a)$	$(1+a)x^3+(1+a)x^2$	$(1+a)x+(1+a)$	$(1+a)x^3+(1+a)x^2+(1+a)x+(1+a)$

Table 5.3.4b Message and codewords of (4,2) polynomial code of Example 5.3.4

\mathbb{Z}_2^2					
u		y			
(00	00)	(00	00	00	00)
(00	10)	(00	10	11	10)
(00	01)	(00	01	11	01)
(00	11)	(00	11	00	11)
(10	00)	(10	00	10	11)
(01	00)	(01	00	01	11)
(11	00)	(11	00	11	00)
(10	10)	(10	10	01	01)
(10	01)	(10	01	01	10)
(10	11)	(10	11	10	00)
(01	10)	(01	10	10	01)
(01	01)	(01	01	10	10)
(01	11)	(01	11	01	00)
(11	10)	(11	10	00	10)
(11	01)	(11	01	00	01)
(11	11)	(11	11	11	11)

constitutes a generator matrix of the systematic (4,2) polynomial code over $P_2^2[a^2+1]$ with generating polynomial $ax^2+(1+a)x+a$. The first 2 symbols are the message symbols.

Case (ii) : g_0 is a unit in $P_p^n[W(a)]$.

The generation of systematic code in this case is similar to the previous case. The message polynomial $u(x)$ is treated as an element of formal power series. $u(x)$ is divided by $g(x)$, using a $P_p^n[W(a)]$ -LSS of order maximum of (K,r) , in K steps. If we denote the remainder at the K th step by $R^{(K)}(x)$, then $u(x)-R^{(K)}(x)$ is a multiple of $g(x)$ and constitutes the codeword polynomial corresponding to the message polynomial $u(x)$.

In the following we assume $r > K-1$. However, the result holds good for any general case by appropriately taking $g_j=0$ for $j > r$. We perform the long division of $u(x)=u_0+u_1x + \dots u_{K-1}x^{K-1}$ by $g(x) = g_0+g_1x + \dots g_r x^r$. The quotient $q^{(i)}(x)$ and remainder $R^{(i)}(x)$ at the i th step are tabulated in Table 5.3.5.

We note that degree of $q^{(i)}(x)$ is less than or equal to $(i-1)$ and degree of $R^{(i)}(x)$ is greater than $(i-1)$ and less than or equal to $(i+r-1)$. The division process is continued upto K steps. In each step the following relations are valid.

Table 5.3.5 Quotient $q^{(i)}(x)$ and remainder $R^{(i)}(x)$ in the division of $u(x)$ by $g(x)$

Step No.	Quotient $q^{(i)}(x)$ $=q_0+q_1x+\dots q_{i-1}x^{i-1}$	Remainder $R^{(i)}(x)$ $=R_i x+R_{i+1}x^{i+1}+\dots R_{i+r-1}x^{i+r-1}$
1	$q_0 = g_0^{-1}u_0$	$(u_1 - g_0^{-1}g_1u_0)x+(u_2-g_0^{-1}g_2u_0)x^2+\dots$ $+(u_{K-1}-g_0^{-1}g_{K-1}u_0)x^{K-1}\dots$ $- g_0^{-1}g_r u_0 x^r .$
2	$g_0^{-1}u_0+g_0^{-1}(u_1-g_0^{-1}g_1u_0)x$	$((u_2-g_0^{-1}g_2u_0)-g_0^{-1}g_1(u_1-g_0^{-1}g_1u_0))x^2+\dots$ $\dots+g_0^{-1}g_r(u_1-g_0^{-1}g_1u_0)x^{r+1} .$

$$u(x) = g(x) q^{(1)}(x) + R^{(1)}(x) \quad \text{1st step}$$

$$u(x) = g(x) q^{(2)}(x) + R^{(2)}(x) \quad \text{2nd step}$$

$$\vdots$$

$$u(x) = g(x) q^{(K)}(x) + R^{(K)}(x) \quad \text{Kth step}$$

Consider $y(x) = u(x) - R^{(K)}(x) = g(x) \cdot q^{(K)}(x)$.

Degree of $q^{(K)}(x)$ is less than or equal to $(K-1)$ and degree of $R^{(K)}(x)$ is less than or equal to $(K+r-1) = (N-1)$. Hence $y(x)$ is a polynomial of degree $(N-1)$ or less and it is a multiple of $g(x)$.

$$\text{Further} \quad y_i = u_i \quad i = 0, 1, \dots, (K-1)$$

$$\text{and} \quad y_i = -R_i \quad i = K, \dots, (N-1).$$

Hence the code generated by $g(x)$ is in systematic form. Note that here also the first K symbols are the message symbols. However, they are the coefficients of lower degree terms.

Example 5.3.5 :

Consider $(4,2)$ systematic polynomial code over $P_2^2[a^2+1]$ generated by $g(x) = a+(1+a)x+ax^2$ of Example 5.3.4. The message word, remainder $R^{(2)}(x)$ after division of $u(x)$ by $g(x)$ in two steps and codeword polynomial $y(x) = u(x) - R^{(2)}(x)$ are given in Table 5.3.6. The corresponding message u and codeword y over $Z_2^2 \cong P_2^2[a^2+1]$ are also given.

All the codeword polynomials are multiples of $g(x)$. The codeword polynomials corresponding to message polynomial $u(x) = 1$ and x can be taken as a basis. Then the matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & (1+a) \\ 0 & 1 & (1+a) & 1 \end{bmatrix}$$

Table 5.3.6 Message and codewords of the (4,2) systematic polynomial code of Example 5.3.5

$P_2^2[a^2+1]$			Z_2^2	$\simeq P_2^2[a^2+1]$
$u(x)$	$R^{(2)}(x)$	$y(x)=u(x)-R^{(2)}(x)$	u	y
0	0	0	(00 00)	(00 00 00 00)
1	$x^2+(1+a)x^3$	$1+x^2+(1+a)x^3$	(10 00)	(10 00 10 11)
a	$ax^2+(1+a)x^3$	$a+ax^2+(1+a)x^3$	(01 00)	(01 00 01 11)
1+a	$(1+a)x^2$	$(1+a)+(1+a)x^2$	(11 00)	(11 00 11 00)
x	$(1+a)x^2+x^3$	$x+(1+a)x^2+x^3$	(00 10)	(00 10 11 10)
ax	$(1+a)x^2+ax^3$	$ax+(1+a)x^2+ax^3$	(00 01)	(00 01 11 01)
$(1+a)x$	$(1+a)x^3$	$(1+a)x+(1+a)x^3$	(00 11)	(00 11 00 11)
$(1+x)$	ax^2+ax^3	$1+x+ax^2+ax^3$	(10 10)	(10 10 01 01)
$(a+x)$	x^2+ax^3	$a+x+x^2+ax^3$	(01 10)	(01 10 10 01)
$(1+a)+x$	x^3	$(1+a)+x+x^3$	(11 10)	(11 10 00 10)
1+ax	ax^2+x^3	$1+ax+ax^2+x^3$	(10 01)	(10 01 01 10)
a+ax	x^2+x^3	$a+ax+x^2+x^3$	(01 01)	(01 01 10 10)
$(1+a)+ax$	ax^3	$(1+a)+ax+ax^3$	(11 01)	(11 01 00 01)
$1+(1+a)x$	x^2	$1+(1+a)x+x^2$	(10 11)	(10 11 10 00)
$a+(1+a)x$	ax^2	$a+(1+a)x+ax^2$	(01 11)	(01 11 01 00)
$(1+a)+$ $(1+a)x$	$(1+a)x^2+$ $(1+a)x^3$	$(1+a)+(1+a)x+$ $(1+a)x^2+(1+a)x^3$	(11 11)	(11 11 11 11)

constitutes a generator matrix of the systematic (4,2) polynomial code over $P_2^2[a^2+1]$ generated by $g(x) = a+(1+a)x+ax^2$. The first two symbols are the message symbols. In the preceeding two examples both g_0 and g_1 are units. In the following we consider another example with g_0 a unit and g_1 a zero divisor in $P_2^2[a^2+1]$.

Example 5.3.6 :

Consider (4,2) polynomial code generated by $g(x) = a+(1+a)x+(1+a)x^2$ over $P_2^2[a^2+1]$. The message polynomial $u(x)$, the remainder $R^{(2)}(x)$ after division of $u(x)$ by $g(x)$ in two steps and codeword polynomial $y(x) = u(x)-R^{(2)}(x)$ are given in Table 5.3.7. The corresponding message \underline{u} and codeword \underline{y} over $Z_2^2 \cong P_2^2[a^2+1]$ are also given.

All the codeword polynomials are multiples of $g(x)$. The codeword polynomials corresponding to message polynomial $u(x)=1$ and $u(x) = x$ can be taken as basis. Then the matrix

$$G = \begin{bmatrix} 1 & 0 & 1+a & 0 \\ 0 & 1 & 0 & 1+a \end{bmatrix}$$

constitutes a generator matrix of the systematic (4,2) polynomial code over $P_2^2[a^2+1]$ generated by $g(x) = a+(1+a)x+(1+a)x^2$. The first two symbols are the message symbols, which are the coefficients of the lower degree terms. We note that the minimum weight of the code is one.

Table 5.3.7 Message and codewords of (4,2) systematic polynomial code of Example 5.3.6

$P_2^2[a^2+1]$			$Z_2^2 \simeq P_2^2[a^2+1]$	
$u(x)$	$R^{(2)}(x)$	$y(x)=u(x)-R^{(2)}(x)$	u	y
0	0	0	00 00	(00 00 00 00)
1	$(1+a)x^2$	$1+(1+a)x^2$	(10 00)	(10 00 11 00)
a	$(1+a)x^2$	$a+(1+a)x^2$	(01 00)	(01 00 11 00)
$(1+a)$	0	$(1+a)$	(11 00)	(11 00 00 00)
x	$(1+a)x^3$	$x+(1+a)x^3$	(00 10)	(00 10 00 11)
ax	$(1+a)x^3$	$ax+(1+a)x^3$	(00 01)	(00 01 00 11)
$(1+a)x$	0	$(1+a)x$	(00 11)	(00 11 00 00)
$(1+x)$	$(1+a)x^2+$ $(1+a)x^3$	$1+x+(1+a)x^2+$ $(1+a)x^3$	(10 10)	(10 10 11 11)
$a+x$	$(1+a)x^2+$ $(1+a)x^3$	$a+x+(1+a)x^2+$ $(1+a)x^3$	(01 10)	(01 10 11 11)
$(1+a)+x$	$(1+a)x^3$	$(1+a)+x+(1+a)x^3$	(11 10)	(11 10 00 11)
$1+ax$	$(1+a)x^2+$ $(1+a)x^3$	$1+ax+(1+a)x^2+$ $(1+a)x^3$	(10 01)	(10 01 11 11)
$a+ax$	$(1+a)x^2+$ $(1+a)x^3$	$a+ax+(1+a)x^2+$ $(1+a)x^3$	(01 01)	(01 01 11 11)
$(1+a)+ax$	$(1+a)x^3$	$(1+a)+ax+(1+a)x^3$	(11 01)	(11 01 00 11)
$1+(1+a)x$	$(1+a)x^2$	$1+(1+a)x+(1+a)x^2$	(10 11)	(10 11 11 00)
$a+(1+a)x$	$(1+a)x^2$	$a+(1+a)x+(1+a)x^2$	(01 11)	(01 11 11 00)
$(1+a)+$ $(1+a)x$	0	$(1+a)+(1+a)x$	(11 11)	(11 11 00 00)

5.3.2 Minimum Distance Properties

The minimum distance of an (N, K) polynomial code over $P_p^n[W(a)]$ depends on the generator polynomial $g(x)$. For a general $g(x)$ the following theorem holds which is a variation of a theorem proved for codes over $GF(2)$ in [65].

Theorem 5.3.4 :

Consider a $g(x)$ of degree $r \geq 1$ over $P_p^n[W(a)]$. If g_0 and g_r are units and $g(x)$ does not divide any polynomial of the form $(y_{i1} + y_{i2}x^j)$ for $j < N$; $N \geq 3$, then the code generated by $g(x)$ has minimum distance at least 3.

Proof :

It is seen in Lemma 5.2.1 that the necessary condition for the minimum distance to be at least 3 is that $N \geq 3$.

The code generated by $g(x)$ is the set of all polynomials $g(x) \cdot u(x)$, degree of $u(x)$ is less than K . In a linear code the minimum distance between codewords is equal to the minimum weight of some codeword. In order to show that the minimum weight is 3, we show there is no codeword of weight 1 or 2.

If there is a codeword of weight 1, then there exists $y_j x^j$, $j \leq (N-1)$, such that $g(x)$ divides $y_j x^j$. But $g(x)$ is of degree $r \geq 1$ and with g_0, g_r units. Hence $g(x)$ does not divide polynomials of the form $y_j x^j$, $j \leq (N-1)$. Therefore there are no codewords of weight 1.

If there is a codeword of weight 2, then $y(x)$ will have only two terms $y(x) = y_{i_1} x^{i_1} + y_{i_2} x^{i_2}$, $i_1, i_2 \leq (N-1)$

$$= x^{i_1} (y_{i_1} + y_{i_2} x^{i_2 - i_1})$$

and $g(x)$ should divide $y(x)$. Since g_0 is a unit $g(x)$ should divide $(y_{i_1} + y_{i_2} x^{i_2 - i_1})$. But $g(x)$ divides no polynomial of the form $(y_{i_1} + y_{i_2} x^j)$ for $j < N$. Therefore, $g(x)$ does not divide $y(x)$ and there are no codewords with weight 2.

Example 5.3.7 :

Consider a $(6,2)$ polynomial code over $P_2^2[a^2+1]$ generated by $g(x) = a+ax+(1+a)x^2+ax^3+x^4$ we have $g_0 = a$ and $g_4 = 1$. Therefore, codewords have degree ≥ 4 . We examine whether $g(x)$ divides $(y_{i_1} + y_{i_2} x^j)$ for $j < 6$. We check this without doing long division.

Suppose $g(x) | (y_{i_1} + y_{i_2} x^j)$, then $y_{i_2} x^j = -y_{i_1}$ modulo $[2; g(x)]$

We have $g(x) \equiv 0$ modulo $[2; g(x)]$

$$x^4 = a+ax+(1+a)x^2+ax^3 \text{ modulo } [2; g(x)]$$

$$x^5 = 1+(1+a)x+ax^2+ax^3 \text{ modulo } [2; g(x)]$$

$$x^6 = 1 \text{ modulo } [2; g(x)]$$

Therefore, $g(x) | (x^6 - 1)$.

Hence from the result of Theorem 5.3.4, the minimum weight is at least 3. The codewords and their weights are tabulated in Table 5.3.8 from which it is seen that the minimum distance of the code is 4.

The generator matrix of this polynomial code is

$$G = \begin{bmatrix} a & a & 1+a & a & 1 & 0 \\ 0 & a & a & 1+a & a & 1 \end{bmatrix}$$

G is not in canonical form. There are 16 possible linear combinations of the two rows of G which constitute the code.

Example 5.3.8 :

Let $g(x) = a + (1+a)x + ax^2$ over $P_2^2[a^2+1]$ and

Let $u(x)$ be of degree 2.

Then $g(x)$ generates a (5,3) polynomial code over $P_2^2[a^2+1]$.

$$ax^2 = (1+a)x + a \pmod{g(x)}$$

$$\text{and } (1+a)x^2 = (1+a) \pmod{g(x)}$$

$$\text{Therefore, } g(x) \mid ((1+a)x^2 + (1+a))$$

$g(x)$ divides a polynomial of two terms whose degree is less than 5. Hence the minimum weight is less than 3, as per Theorem 5.3.4. There are totally 64 code polynomials. We donot write all the code polynomials but pick one which has weight less than 3 to illustrate the theorem.

Table 5.3.8: Code words of (6,2) linear polynomial code of Example 5.3.7.

Message word $u(x)$	Code word $y(x)$	\underline{u}	\underline{y}	Weight
0 0	0 0 0 0 0 0	00 00	00 00 00 00 00 00	0
0 1	0 a a $1+a$ a 1	00 10	00 01 01 11 01 10	5
0 a	0 1 1 $1+a$ 1 a	00 01	00 10 10 11 10 01	5
0 $1+a$	0 $1+a$ $1+a$ 0 $1+a$ $1+a$	00 11	00 11 11 00 11 11	4
1 0	a a $1+a$ a 1 0	10 00	01 01 11 01 10 00	5
1 1	a 0 1 1 $1+a$ 1	10 10	01 00 10 10 11 10	5
1 a	a $1+a$ a 1 0 a	10 01	01 11 01 10 00 01	5
1 $1+a$	a 1 0 a a $1+a$	10 11	01 10 00 01 01 11	5
a 0	1 1 $1+a$ 1 a 0	01 00	10 10 11 10 01 00	5
a 1	1 $1+a$ 1 a 0 1	01 10	10 11 10 01 00 10	5
a a	1 0 a a $1+a$ a	01 01	10 00 01 01 11 01	5
a $1+a$	1 a 0 1 1 $1+a$	01 11	10 01 00 10 10 11	5
$1+a$ 0	$1+a$ $1+a$ 0 $1+a$ $1+a$ 0	11 00	11 11 00 11 11 00	4
$1+a$ 1	$1+a$ 1 a 0 1 1	11 10	11 10 01 00 10 10	5
$1+a$ a	$1+a$ a 1 0 a a	11 01	11 01 10 00 01 01	5
$1+a$ $1+a$	$1+a$ 0 $1+a$ $1+a$ 0 $1+a$	11 11	11 00 11 11 00 11	4

The (N, K) polynomial code C of order p^{nK} is a submodule in the module V of order p^{nN} . A module is an additive Abelian group. Hence cosets of C in V can be formed. The number of cosets is equal to $p^{n(N-K)}$. The number of terms in the remainder is $r = (N-K)$. Therefore, the number of distinct syndromes is $p^{n(N-K)}$.

We show below that two polynomials having the same remainder on division by $g(x)$ are in the same coset.

Theorem 5.3.5 :

Two polynomials $v_1(x)$ and $v_2(x)$ of degree $\leq (N-1)$ having the same syndrome are in the same coset of the (N, K) polynomial code C over $P_p^n[W(a)]$ in the Abelian group of all polynomials of degree $\leq (N-1)$ over $P_p^n[W(a)]$.

Proof :

$$\text{Let } v_1(x) = g(x) q(x) + R(x)$$

$$\text{and } v_2(x) = g(x) q'(x) + R(x) .$$

$$\text{Then } v_1(x) - v_2(x) = g(x) \cdot [q(x) - q'(x)]$$

is a multiple of $g(x)$, is of degree $\leq (N-1)$, and therefore is a code polynomial belonging to C . As seen in Section 2.1, from the property of the elements in the cosets, it implies that $v_1(x)$ and $v_2(x)$ are in the same coset.

$$\text{Let } u(x) = (1+a) + 0.x + 0.x^2$$

Then the corresponding code polynomial is

$$y(x) = (1+a) + (1+a)x^2$$

Corresponding codeword is $((1+a), 0, (1+a), 0)$.

Hence minimum weight is less than 3.

5.3.3 Decoding Principles

The error detection using an (N,K) polynomial code generated by $g(x)$ is done by computing the syndrome of the received polynomial $y'(x)$. Codewords in a polynomial code are multiples of $g(x)$ which gives a straightforward syndrome computation. It is the remainder after division by $g(x)$ of the received polynomial $y'(x)$. If there is no error, $y'(x)$ being a codeword polynomial, on division by $g(x)$ the remainder (syndrome) is zero. Because of channel noise $y'(x)$ may be different from the transmitted codeword polynomial. In this case division by $g(x)$ results in a nonzero remainder (syndrome).

At the decoder it must be known whether the codeword symbols, treated as coefficients of $y(x)$ are in the ascending order of powers of x or in the descending order of powers of x . In the former case $y(x)$ is treated as a polynomial and for implementing division by $g(x)$, g_r must necessarily be a unit in $P_p^n[W(a)]$. In the latter case $y(x)$ is treated as a formal power series and for implementing division by $g(x)$, g_0 must necessarily be a unit in $P_p^n[W(a)]$.

The (N, K) polynomial code C of order p^{nK} is a submodule in the module V of order p^{nN} . A module is an additive Abelian group. Hence cosets of C in V can be formed. The number of cosets is equal to $p^{n(N-K)}$. The number of terms in the remainder is $r = (N-K)$. Therefore, the number of distinct syndromes is $p^{n(N-K)}$.

We show below that two polynomials having the same remainder on division by $g(x)$ are in the same coset.

Theorem 5.3.5 :

Two polynomials $v_1(x)$ and $v_2(x)$ of degree $\leq (N-1)$ having the same syndrome are in the same coset of the (N, K) polynomial code C over $P_p^n[W(a)]$ in the Abelian group of all polynomials of degree $\leq (N-1)$ over $P_p^n[W(a)]$.

Proof :

$$\text{Let } v_1(x) = g(x) q(x) + R(x)$$

$$\text{and } v_2(x) = g(x) q'(x) + R(x) .$$

$$\text{Then } v_1(x) - v_2(x) = g(x) \cdot [q(x) - q'(x)]$$

is a multiple of $g(x)$, is of degree $\leq (N-1)$, and therefore is a code polynomial belonging to C . As seen in Section 2.1, from the property of the elements in the cosets, it implies that $v_1(x)$ and $v_2(x)$ are in the same coset.

From the above theorem it is seen that each coset corresponds to a distinct syndrome as in the case of linear block codes. The error correction is done by using the decoding table which consists of all possible syndromes and the corresponding minimum weight polynomials. If $y'(x)$ is the received polynomial its syndrome $s(y')$ is computed. The corresponding minimum weight polynomial $e(x)$ is subtracted from $y'(x)$ to get $\hat{y}(x)$, which is the most likely transmitted codeword polynomial.

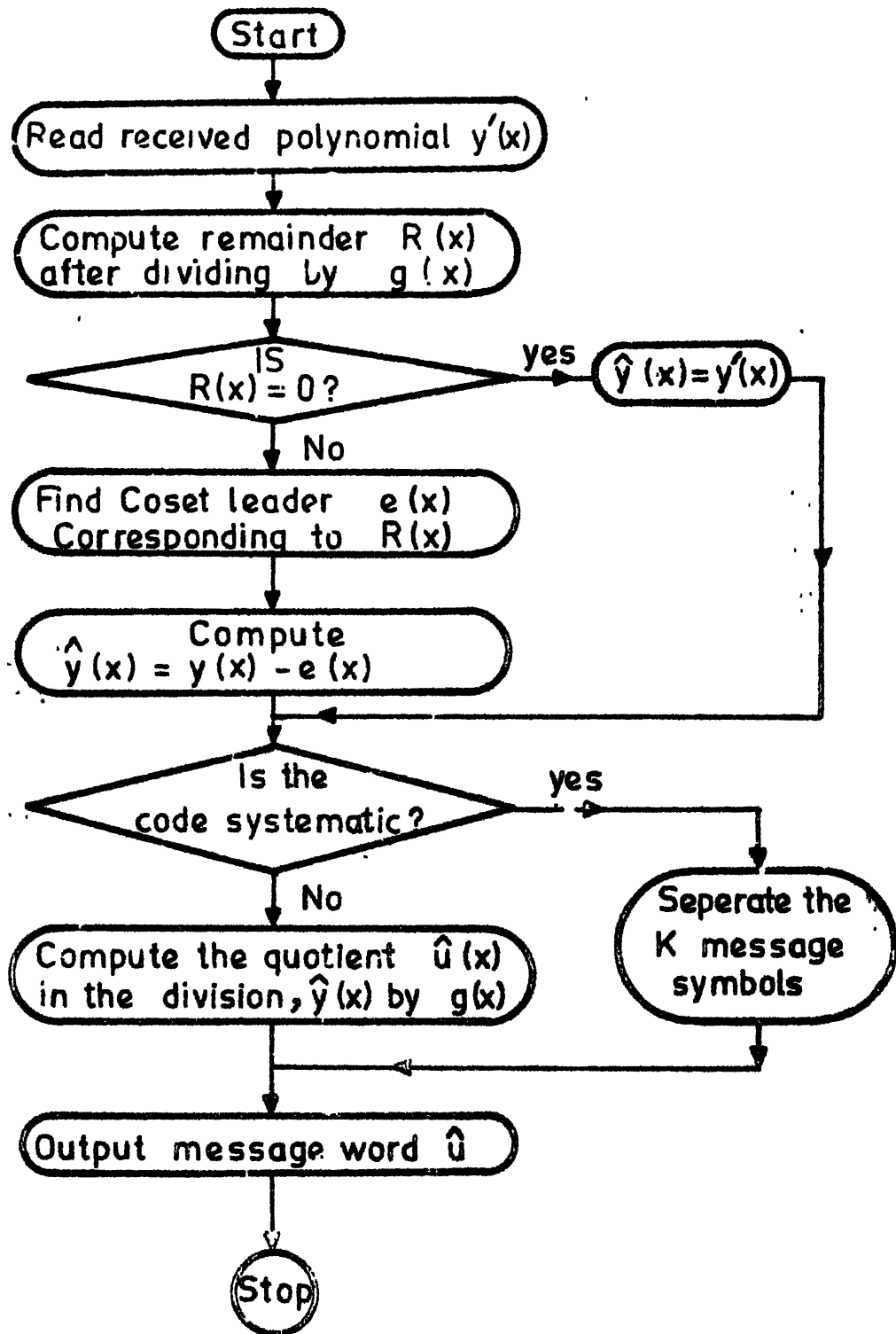
The decoding procedure is given in Flow Chart 5.3.1.

Example 5.3.9 :

We consider the single error correcting (3,1) polynomial code C over $P_2^2[a^2+1]$, of Example 5.3.3 generated by $g(x) = a+x+ax^2$. The message and codeword polynomials are given in Table 5.3.3. We form the cosets of C in the group of all polynomials of degree 2 over $P_2^2[a^2+1]$. For the sake of convenience we write the polynomials as 3-tuples. For example $a+x+ax^2$ will be written as $(a \ 1 \ a)$. The cosets and the associated syndromes are given in Table 5.3.9.

Suppose the received polynomial $y'(x)$ is $1+ax+ax^2$. From Table 5.3.9, the syndrome of $y'(x)$ is $(1+a)+(1+a)x$, and the associated coset leader $e(x)$ is $(1+a)x^2$. Therefore the most likely transmitted polynomial is

$$\begin{aligned}\hat{y}(x) &= y'(x) - e(x) \\ &= (1+ax+ax^2) - (1+a)x^2 \\ &= (1+ax+x^2).\end{aligned}$$



Flow Chart .5.3.1 Decoding Procedure for Polynomial Codes

Table 5.3.9: Coset table and the associated syndromes
of the (3,1) polynomial code of Example 5.3.9.

Coset leaders	Cosets									Syndromes
0 0 0	a	1	a	1	a	1	1+a	1+a	1+a	0 0
0 0 1	a	1	1+a	1	a	0	1+a	1+a	a	1 a
0 0 a	a	1	0	1	a	1+a	1+a	1+a	1	a 1
0 0 1+a	a	1	1	1	a	a	1+a	1+a	0	1+a 1+a
0 1 0	a	0	a	1	1+a	1	1+a	a	1+a	0 1
0 a 0	a	1+a	a	1	0	1	1+a	1	1+a	0 a
0 1+a 0	a	a	a	1	1	1	1+a	0	1+a	0 1+a
1 0 0	1+a	1	a	0	a	1	a	1+a	1+a	1 0
a 0 0	0	1	a	1+a	a	1	1	1+a	1+a	a 0
1+a 0 0	1	1	a	a	a	1	0	1+a	1+a	1+a 0
0 1 1	a	0	1+a	1	1+a	0	1+a	a	a	1 1+a
0 1 1+a	a	0	1	1	1+a	a	1+a	a	0	(1+a) a
0 a a	a	1+a	0	1	0	1+a	1+a	1	1	a (1+a)
0 a 1+a	a	1+a	1	1	0	a	1+a	1	0	1+a 1
0 1+a 1	a	a	1+a	1	1	0	1+a	0	a	1 1
0 1+a a	a	a	0	1	1	1+a	1+a	0	1	a a

Having studied the properties, encoding and decoding of polynomial codes over $P_p^n[W(a)]$, in the next section we take up the study of linear cyclic codes over $P_p^n[W(a)]$ which constitute a specific class of polynomial codes studied in this section.

5.4 LINEAR CYCLIC CODES OVER $P_p^n[W(a)]$

In an (N,K) polynomial code generated by $g(x)$ of degree $r = (N-K)$, the code polynomials $g(x), xg(x), \dots, x^{K-1}g(x)$ are cyclic shifts of $g(x)$. But cyclic shift of every codeword is not necessarily a codeword. Linear cyclic codes are a subclass of polynomial codes (as defined in the previous section), with additional restriction on $g(x)$ to guarantee that cyclic shift of every codeword is also a codeword. Linear cyclic codes are thus a special case of linear block codes in which cyclic shift of every codeword is also a codeword. Since a linear block code over $P_p^n[W(a)]$ is a module, linear cyclic codes over $P_p^n[W(a)]$ are closed under addition and scalar multiplication in $P_p^n[W(a)]$, and cyclic shifts. In what follows, by cyclic code we mean linear cyclic code.

5.4.1 Generating Polynomial, Generator Matrix and Encoding Principles

As seen in the previous section, if the generating polynomial $g(x)$ of an (N,K) polynomial code over $P_p^n[W(a)]$ has either g_0 or g_r a unit in $P_p^n[W(a)]$ there is a one-to-one correspondence between the message and codeword polynomials and decoding is unambiguous.

For the polynomial code to be a cyclic code cyclic shift of every codeword must also be a codeword. This puts additional restriction on $g(x)$ enunciated in the following theorem.

Theorem 5.4.1 :

An (N, K) polynomial code C over $P_p^n[W(a)]$ generated by $g(x) = g_0 + g_1x + \dots + g_rx^r$, is a cyclic code iff g_0 and g_r are units in $P_p^n[W(a)]$ and $g(x)$ divides $(x^N - 1)$.

Proof :

We first prove that if C is an (N, K) cyclic code generated by $g(x)$ of degree $r = N - K$ then $g(x)$ divides $(x^N - 1)$ and g_0 and g_r must be units in $P_p^n[W(a)]$.

Consider $y(x) = x^{K-1}g(x) = g_0x^{K-1} + g_1x^K + \dots + g_rx^{K+r-1}$ which is a codeword polynomial. The cyclic shift $\sigma y(x)$ of the codeword $y(x)$, i.e.,

$$\begin{aligned} y'(x) = \sigma y(x) &= g_0x^K + g_1x^{K+1} + \dots + g_{r-1}x^{K+r-1} \quad (5.4.1) \\ &= x^K g(x) - g_r(x^N - 1) \text{ is also a codeword.} \end{aligned}$$

Since all the codewords are multiples of $g(x)$, $g(x)$ divides $y'(x)$. Hence it should divide the right hand side of Equation (5.4.1). Therefore, $g(x)$ should divide $g_r(x^N - 1)$.

This implies that there exists a polynomial

$h'(x) = h'_0 + h'_1x + \dots + h'_kx^k$ of degree k over $P_p^n[W(a)]$ such that $g(x).h'(x) = g_r(x^N - 1)$.

Equating the coefficients of like powers on both sides, the following equations must necessarily be satisfied.

Coefficient of x^N : $g_r h'_K = g_r$ therefore $h'_K = g_r^{-1} g_r$

Coefficient of x^{N-1} : $g_{r-1} h'_K + g_r h'_{K-1} = 0$ therefore,

$$h'_{K-1} = -g_r^{-1} g_{r-1} h'_K$$

\vdots

Coefficient x : $g_1 h'_0 + g_0 h'_1 = 0$ therefore $h'_1 = -g_0^{-1} g_1 h'_0$

Coefficient of x^0 : $g_0 h'_0 = g_0$ therefore $h'_0 = g_0^{-1} g_0$

Thus g_r and g_0 must necessarily be units.

We now prove that if g_0 and g_r are units in $P_p^n[W(a)]$ and if $g(x)$ divides (x^N-1) , then the polynomial code generated by $g(x)$ is an (N, K) cyclic code.

Let $y(x) = y_0 + y_1 x + \dots + y_{N-1} x^{N-1}$ be a codeword polynomial in the polynomial code generated by $g(x)$. Therefore, $g(x)$ divides $y(x)$. The cyclic shift of the codeword $y(x)$ is

$$\begin{aligned} \sigma y(x) &= y_{N-1} + y_0 x + y_1 x^2 + \dots + y_{N-2} x^{N-1} \\ &= xy(x) - y_{N-1}(x^N - 1) \end{aligned}$$

Since $g(x)$ divides $y(x)$ and $g(x)$ divides (x^N-1) it follows that $g(x)$ divides $\sigma y(x)$.

In a polynomial code every codeword is a multiple of $g(x)$. Here $y(x)$ is a multiple of $g(x)$ and cyclic shift of $y(x)$ is also multiple of $g(x)$. This implies that if $y(x)$ is a codeword its cyclic shift is also a codeword. Therefore, the code C is cyclic.

*

We note here that the theorem also holds good for the case when codewords are expressed as $y = (y_{N-1} y_{N-2} \dots y_1 y_0)$. However, in this case the cyclic shift is in the reverse sense i.e. left cyclic shift.

In the case of generating polynomial of (N, K) polynomial codes over $P_p^n[W(a)]$ it is enough if either g_0 or g_r is a unit in $P_p^n[W(a)]$. The encoding and decoding can be done unambiguously. However, in the case of (N, K) cyclic codes the coefficients g_0 and g_r of $g(x)$ must both be units in $P_p^n[W(a)]$ and further $g(x)$ must divide $(x^N - 1)$.

If $y(x)$ is a codeword in a cyclic code then $\sigma^1 y(x)$, cyclic shift of $y(x)$ by 1 places can also be expressed as $x^1 y(x)$ modulo $(x^N - 1)$. Since every codeword is a multiple of $g(x)$ we have the following.

Theorem 5.4.2 :

The (N, K) cyclic code C , generated by $g(x)$ is a principal ideal generated by $g(x)$ in the residue class ring of polynomials over $P_p^n[W(a)]$ modulo $(x^N - 1)$.

Proof :

Let R be the residue class ring of polynomials over $P_p^n[W(a)]$ modulo (x^N-1) . For C to be an ideal in R , C must be a subset of R which is an additive subgroup and for every $Z(x) \in R$ and $y(x) \in C$, $z(x) \cdot y(x)$ modulo (x^N-1) must be in C .

Since C is a linear code, it is an additive subgroup of R that is for $y(x), v(x) \in C$, $y(x) \pm v(x) \in C$.

Let $z(x) = \sum_{i=0}^{N-1} z_i x^i$ be any arbitrary element of R

$z(x) \cdot y(x)$ modulo $(x^N-1) = z_0 y(x) + z_1 x y(x) + \dots + z_{N-1} x^{N-1} y(x)$ modulo (x^N-1) is a linear combination of cyclic shifts of $y(x)$ and hence is a codeword. Therefore, $z(x) \cdot y(x)$ modulo $(x^N-1) \in C$.

Hence, C is an ideal in R ; $g(x)$ is the least degree polynomial in C and every element of C is a multiple of $g(x)$. Therefore, C is a principal ideal generated by $g(x)$. *

With the restriction that g_r a unit there may be more than one codeword polynomial in C whose degree is r and constant term is a unit. That is any polynomial of degree r with coefficients y_0, y_r units in $P_p^n[W(a)]$, may be regarded as the generator of the ideal. The generator of the ideal can be made unique by putting the restriction that $g(x)$ is monic.

Thus an (N, K) cyclic code C over $P_p^n[W(a)]$ can be regarded as an (N, K) polynomial code generated by a unique monic polynomial $g(x)$ of degree $r = (N-K)$ with g_0 a unit such that $g(x)$

divides (x^N-1) . Further in the ring R of polynomials over $P_p^n[W(a)]$ modulo (x^N-1) , C is the principal ideal generated by $g(x)$.

Generator Matrix :

Just as in the case of polynomial codes, an (N,K) cyclic code C over $P_p^n[W(a)]$, generated by $g(x)$, can also be described by its generator matrix G whose first row consists of the coefficients of $g(x)$ and the succeeding rows are the cyclic shifts of the preceding rows. Thus the generator matrix of an (N,K) cyclic code over $P_p^n[W(a)]$ can be seen as a $K \times N$ matrix of the following form :

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & & & 0 \\ \vdots & & & & & & & \\ 0 & 0 & & g_0 & g_1 & & & g_n \end{bmatrix} \quad (5.4.2)$$

Now since $g(x)$ divides (x^N-1) , we have a polynomial $h(x)$ of degree K such that

$$g(x) \cdot h(x) = 0 \text{ modulo } [p; (x^N-1)]$$

where $g_r \cdot h_k = 1$. Since every codeword $y(x)$ is a multiple of $g(x)$,

$$h(x) \cdot y(x) = 0 \text{ modulo } [p; (x^N-1)] .$$

Let $h(x) = h_0 + h_1x + h_2x^2 + \dots + h_{K-1}x^{K-1} + h_Kx^K$, whose coefficients specify the $(N-K) \times N$ check matrix

$$H = \begin{bmatrix} 0 & 0 & \dots & 0 & h_K & h_{K-1} & \dots & h_2 & h_1 & h_0 \\ 0 & 0 & \dots & 0 & h_K & h_{K-1} & & h_2 & h_1 & h_0 & 0 \\ \vdots & & & & & & & & & & \\ h_K & h_{K-1} & & h_2 & h_1 & h_0 & 0 & 0 & \dots & \dots & 0 \end{bmatrix} \quad (5.4.3)$$

of the linear cyclic code generated by $g(x)$. If $g_r = 1$ we have $h_K = 1$. We note here that codeword y is represented by $(y_0 \ y_1 \ y_2 \ \dots \ y_{N-1})$.

Likewise a $K \times N$ generator matrix with first row $(g_r \ g_{r-1} \ \dots \ g_1 \ g_0 \ 0 \ \dots \ 0)$ and the corresponding $(N-K) \times N$ check matrix with first row given by $(0 \ 0 \ \dots \ 0 \ h_0 \ h_1 \ \dots \ h_{K-1} \ h_K)$ are associated with a cyclic code where a codeword y is represented by $y = (y_{N-1} \ y_{N-2} \ \dots \ y_1 \ y_0)$.

Encoding Principles :

Encoding of cyclic codes is based on the fact that every codeword is a multiple of the generating polynomial $g(x)$. If $u(x)$ is the message word polynomial then $u(x) \cdot g(x)$ is the codeword polynomial. As in the case of polynomial codes discussed in the previous section two implementations are possible based on g_r or g_0 being a unit. The code generated in this manner is not in systematic form. Systematic cyclic codes are generated in the same manner as the systematic polynomial codes

discussed in Section 5.3. There are two implementations based on (i) g_r a unit and (ii) g_o a unit. In case (i) $u(x) = u_{K-1}x^{K-1} + \dots + u_1x + u_0$ is multiplied by x^{N-K} which is then divided by $g(x)$ to give a quotient $q(x)$ and remainder $R(x)$. Thus $x^{(N-K)} u(x) = g(x).q(x) + R(x)$ and $y(x) = x^{(N-K)} u(x) - R(x) = g(x).q(x)$ is a multiple of $g(x)$ and hence is a codeword polynomial corresponding to $u(x)$. The message polynomial, and the codeword polynomial are expressed in descending powers of x . The first K symbols correspond to the message symbols. In case (ii) the message word polynomial $u(x) = u_0 + u_1x + \dots + u_{K-1}x^{K-1}$ is treated as a formal power series. $u(x)$ is divided by $g(x)$ in K steps to obtain a quotient $q^{(K)}(x)$ and remainder $R^{(K)}(x)$. Then $u(x) = g(x).q^{(K)}(x) + R(x)$ and $y(x) = u(x) - R^{(K)}(x) = g(x).q^{(K)}(x)$ is a multiple of $g(x)$ and is the codeword polynomial corresponding to $u(x)$.

A third method of generating an (N,K) systematic cyclic code is based on the following theorem.

Theorem 5.4.3 :

The set C of all autonomous responses of periodic length N of a nonsingular, single output canonical LSS over $P_p^n[W(a)]$ with matrix $C = [1 \ 0 \ \dots \ 0]$ constitutes an (N,K) cyclic code over $P_p^n[W(a)]$.

Proof :

We have to prove that the set of all autonomous responses

of length N (i) is closed under addition. Scalar multiplication and cyclic shift and (ii) if the response is expressed as a polynomial $y(x)$ of degree less than or equal to $(N-1)$, then $y(x)$ is a multiple of a fixed polynomial $g(x)$.

Let $y = (y_0, y_1, \dots, y_{N-1})$ be the autonomous response with the initial state x_0 and $z = (z_0, z_1, \dots, z_{N-1})$ be the autonomous response with the initial state x'_0 . Then the autonomous response

$$\alpha(y_0, y_1, \dots, y_{N-1}) + \beta(z_0, z_1, \dots, z_{N-1}) = (\alpha y_0 + \beta z_0, \alpha y_1 + \beta z_1, \dots, \alpha y_{N-1} + \beta z_{N-1})$$

corresponds to the initial state $\alpha x_0 + \beta x'_0$, where

where $\alpha, \beta \in P_p^n[W(a)]$. Thus the set of autonomous responses of length N constitutes a linear code.

The autonomous response $(y_{N-1}, y_0, \dots, y_{N-2})$, cyclic shift of y is the response to the initial state $A^{N-1}x_0 = A^{-1}x_0$ (N is multiple of period of A) as given in Section 4.3. Hence C is closed under cyclic shifts.

Let $f(x)$ be the feedback polynomial of the nonsingular LSS then as seen in Section 4.3, there exists a $g(x)$ and integer N such that $f(x) \cdot g(x) = (1-x^N)$. The generating function of the autonomous response is

$$y'(x) = \frac{u'(x)}{f(x)} = \frac{u'(x)g(x)}{(1-x^N)} = u'(x) g(x)[1+x^N+x^{2N}+\dots]. \text{ If we}$$

consider polynomial $y(x) = u'(x) g(x)$ of degree $\leq (N-1)$ then the sequence of coefficients $(y_0, y_1 \dots y_{N-1})$ constitutes the autonomous response of the LSS. Further $y(x)$ is a multiple of $g(x)$.

The set of autonomous responses is hence closed under addition and multiplication by scalars in $P_p^n[W(a)]$, and cyclic shifts. Further, responses, if expressed as polynomials, are multiples of a fixed polynomial $g(x)$. Hence the set constitutes a linear cyclic code. *

Thus for the generation of an (N,K) systematic cyclic codes, using a $P_p^n[W(a)]$ -LSS, the K message symbols are the initial state of a single output nonsingular canonical LSS with matrix $C = [1 \ 0 \ \dots \ 0]$. The corresponding autonomous response of length N is the codeword. This point of view of cyclic codes over finite fields is given in [17].

Example 5.4.1 :

Consider the $(6,2)$ polynomial code of Example 5.3.7 generated by $g(x) = a+ax+(1+a)x^2+ax^3+x^4$ over $P_2^2[a^2+1]$. As seen in Example 5.3.7 $g(x)$ divides (x^6-1) . Hence the code is cyclic code. The codewords over $P_2^2[a^2+1]$ and Z_2^2 isomorphic to $P_2^2[a^2+1]$ are listed in Table 5.3.8. We observe that the codewords are $(0 \ 0 \ 0 \ 0 \ 0 \ 0)$, $(0 \ 1 \ 1 \ (1+a) \ 1 \ a)$, $(1 \ 0 \ a \ a \ 1+a \ a)$, $((1+a) \ 0 \ (1+a) \ (1+a) \ 0 \ (1+a))$ and their cyclic shifts. There are 16 possible codewords. The minimum weight of the code is 4.

Hence the code can correct single errors and detect 3 errors.

The code can be generated as the autonomous response of a non-singular, single output canonical LSS with matrix $C = [1 \ 0]$ and feedback polynomial $f(x) = \frac{(1-x^6)}{g(x)} = a+ax+x^2$. The codewords $(1 \ 0 \ a \ a \ (1+a) \ a)$ and $(0 \ 1 \ 1(1+a) \ 1 \ a)$ are linearly independent and hence can be regarded as a basis which generates the code. These two codewords as the two rows of a 2×6 matrix constitute the G matrix in systematic form.

$$G = \begin{bmatrix} 1 & 0 & a & a & 1+a & a \\ 0 & 1 & 1 & 1+a & 1 & a \end{bmatrix}$$

The corresponding parity check matrix is

$$H = \begin{bmatrix} a & 1 & 1 & 0 & 0 & 0 \\ a & 1+a & 0 & 1 & 0 & 0 \\ 1+a & 1 & 0 & 0 & 1 & 0 \\ a & a & 0 & 0 & 0 & 1 \end{bmatrix}$$

We note that every set of 3 columns of H are linearly independent and some 4 columns are linearly dependent, which implies that the minimum distance of the code is 4.

The set of codewords in a cyclic code depends only on the generator polynomial $g(x)$, independent of the method of generation i.e. systematic or nonsystematic. We illustrate this in the following example.

Example 5.4.2 :

The (6,2) cyclic codes generated by $g(x) = 1+x+(1+a)x^2+x^3+ax^4$ in nonsystematic form generated by polynomial multiplication and systematic form generated by autonomous LSS with $f(x) = 1+x+ax^2$ over $P_2^2[a^2+1]$ are considered. The message polynomials and the corresponding codeword polynomials are listed in Table 5.4.1a. The message and systematic codes generated by polynomial division based on g_o a unit and g_r a unit are listed in Table 5.4.1b. The corresponding message and codewords over Z_2^2 are given in Table 5.4.2a and Table 5.4.2b respectively. (Only one of the nonsystematic form of code is considered.)

With reference to Table 5.4.1a, the codewords of the nonsystematic (6,2) cyclic code listed in second column are $(0\ 0\ 0\ 0\ 0\ 0)$, $(1\ 1(1+a)\ 1\ a\ 0)$, $(a\ a\ (1+a)\ a\ 1,0)$, $((1+a)\ (1+a)\ 0\ (1+a)\ (1+a)\ 0)$ and their cyclic shifts. The codewords of the systematic (6,2) cyclic code listed in third column, generated as the autonomous response of LSS, are $(0\ 0\ 0\ 0\ 0\ 0)$, $(1\ 1(1+a)\ 1\ a\ 0)$, $(a\ a\ (1+a)\ a\ 1\ 0)$, $((1+a)\ (1+a)\ 0\ (1+a)\ (1+a)\ 0)$ and their cyclic shifts. With reference to Table 5.4.1b, the codewords of the systematic (6,2) cyclic code, based on g_o a unit, listed in second column are $(0\ 0\ 0\ 0\ 0\ 0)$, $(1\ 1\ (1+a)\ 1.a\ 0)$, $(a\ a\ (1+a)\ a\ 1\ 0)$, $((1+a)\ (1+a)\ 0\ (1+a)\ (1+a)\ 0)$ and their cyclic shifts. The

Table 5.4.1a: (6,2) cyclic code of Example 5.4.2

u(x)	$g(x) = 1+x+(1+a)x^2+x^3+ax^4$	
	$y(x)=u(x) \cdot g(x)$ Nonsystematic code	Autonomous response of LSS with $f(x)=1+x+ax^2$ systematic Code
0	0	0
1	$1+x+(1+a)x^2+x^3+ax^4$	$1+ax^2+ax^3+(1+a)x^4+ax^5$
a	$a+ax+(1+a)x^2+ax^3+x^4$	$a+x^2+x^3+(1+a)x^4+x^5$
(1+a)	$(1+a)+(1+a)x+(1+a)x^3+(1+a)x^4$	$(1+a)+(1+a)x^2+(1+a)x^3+(1+a)x^5$
x	$x+x^2+(1+a)x^3+x^4+ax^5$	$x+x^2+(1+a)x^3+x^4+ax^5$
ax	$ax+ax^2+(1+a)x^3+ax^4+x^5$	$ax+ax^2+(1+a)x^3+ax^4+x^5$
(1+a)x	$(1+a)x+(1+a)x^2+(1+a)x^4+(1+a)x^5$	$(1+a)x+(1+a)x^2+(1+a)x^4+(1+a)x^5$
1+x	$1+ax^2+ax^3+(1+a)x^4+ax^5$	$1+x+(1+a)x^2+x^3+ax^4$
a+x	$a+(1+a)x+ax^2+x^3+ax^5$	$a+x+ax^3+ax^4+(1+a)x^5$
(1+a)+x	$(1+a)+ax+x^2+ax^4+ax^5$	$(1+a)+x+ax^2+x^4+x^5$
1+ax	$1+(1+a)x+x^2+ax^3+x^5$	$1+ax+x^3+x^4+(1+a)x^5$
a+ax	$a+x^2+x^3+(1+a)x^4+x^5$	$a+ax+(1+a)x^2+ax^3+x^4$
(1+a)+ax	$(1+a)+x+ax^2+x^4+x^5$	$(1+a)+ax+x^2+ax^4+ax^5$
1+(1+a)x	$1+ax+x^3+x^4+(1+a)x^5$	$1+(1+a)x+x^2+ax^3+x^5$
a+(1+a)x	$a+x+ax^3+ax^4+(1+a)x^5$	$a+(1+a)x+ax^2+x^3+ax^5$
(1+a)+(1+a)x	$(1+a)+(1+a)x^2+(1+a)x^3+(1+a)x^5$	$(1+a)+(1+a)x+(1+a)x^3+(1+a)x^4$

Table 5.4.1b: (6,2) Systematic Cyclic Code of Example 5.4.2

$g(x)=1+x+(1+a)x^2+x^3+ax^4$			
Based on g_0 a unit		Based on g_2 a unit	
$u(x)=u_0+u_1x$	$y(x)=y_0+y_1x+\dots+y_4x^4+y_5x^5$	$u(x)=u_1x+u_0$	$y(x)=y_5x^5+y_4x^4+\dots+y_1x+y_0$
0	0	0	0
1	$1+ax^2+ax^3+(1+a)x^4+ax^5$	1	$x^4+ax^3+(1+a)x^2+ax+a$
a	$a+x^2+x^3+(1+a)x^4+x^5$	a	$ax^4+x^3+(1+a)x^2+x+1$
(1+a)	$(1+a)+(1+a)x^2+(1+a)x^3+(1+a)x^5$	(1+a)	$(1+a)x^4+(1+a)x^3+(1+a)x+(1+a)$
x	$x+x^2+(1+a)x^3+x^4+ax^5$	x	$x^5+ax^3+x^2+(1+a)x+1$
ax	$ax+ax^2+(1+a)x^3+ax^4+x^5$	ax	$ax^5+x^3+ax^2+(1+a)x+a$
(1+a)x	$(1+a)x+(1+a)x^2+(1+a)x^4+(1+a)x^5$	(1+a)x	$(1+a)x^5+(1+a)x^3+(1+a)x^2+(1+a)$
1+x	$1+x+(1+a)x^2+x^3+ax^4$	x+1	$x^5+x^4+ax^2+x+(1+a)$
a+x	$a+x+ax^3+ax^4+(1+a)x^5$	x+a	$x^5+ax^4+(1+a)x^3+x^2+ax$
(1+a)+x	$(1+a)+x+ax^2+x^4+x^5$	x+(1+a)	$x^5+(1+a)x^4+x^3+x^2+a$
1+ax	$1+ax+x^3+x^4+(1+a)x^5$	ax+1	$ax^5+x^4+(1+a)x^3+x^2+x$
a+ax	$a+ax+(1+a)x^2+ax^3+x^4$	ax+a	$ax^5+ax^4+x^2+ax+(1+a)$
(1+a)+ax	$(1+a)+ax+x^2+ax^4+ax^5$	ax+(1+a)	$ax^5+(1+a)x^4+ax^3+ax^2+1$
1+(1+a)x	$1+(1+a)x+x^2+ax^3+x^5$	(1+a)x+1	$(1+a)x^5+x^4+x^3+ax+1$
a+(1+a)x	$a+(1+a)x+ax^2+x^3+ax^5$	(1+a)x+a	$(1+a)x^5+ax^4+ax^3+x+a$
(1+a)+(1+a)x	$(1+a)+(1+a)x+(1+a)x^3+(1+a)x^4$	(1+a)x+(1+a)	$(1+a)x^5+(1+a)x^4+(1+a)x^2+(1+a)x$

Table 5.4.2a: (6,2) Cyclic Code over \mathbb{Z}_2^2 of Example 5.4.2

$$g(x) = 1+x+(1+a)x^2+x^3+ax^4$$

u	Nonsystematic code y	Systematic code* y
(00 00)	(00 00 00 00 00 00)	(00 00 00 00 00 00)
(10 00)	(10 10 11 10 01 00)	(10 00 01 01 11 01)
(01 00)	(01 01 11 01 10 00)	(01 00 10 10 11 10)
(11 00)	(11 11 00 11 11 00)	(11 00 11 11 00 11)
(00 10)	(00 10 10 11 10 01)	(00 10 10 11 10 01)
(00 01)	(00 01 01 11 01 10)	(00 01 01 11 01 10)
(00 11)	(00 11 11 00 11 11)	(00 11 11 00 11 11)
(10 10)	(10 00 01 01 11 01)	(10 10 11 10 01 00)
(01 10)	(01 11 01 10 00 01)	(01 10 00 01 01 11)
(11 10)	(11 01 10 00 01 01)	(11 10 01 00 10 10)
(10 01)	(10 11 10 01 00 10)	(10 01 00 10 10 11)
(01 01)	(01 00 10 10 11 10)	(01 01 11 01 10 00)
(11 01)	(11 10 01 00 10 10)	(11 01 10 00 01 01)
(10 11)	(10 01 00 10 10 11)	(10 11 10 01 00 10)
(01 11)	(01 10 00 01 01 11)	(01 11 01 10 00 01)
(11 11)	(11 00 11 11 00 11)	(11 11 00 11 11 00)

* Autonomous response of LSS.

Table 5.4.2a: (6,2) Cyclic Code over \mathbb{Z}_2^2 of Example 5.4.2

$$g(x) = 1+x+(1+a)x^2+x^3+ax^4$$

<u>u</u>	Nonsystematic code <u>y</u>	Systematic code* <u>y</u>
(00 00)	(00 00 00 00 00 00)	(00 00 00 00 00 00)
(10 00)	(10 10 11 10 01 00)	(10 00 01 01 11 01)
(01 00)	(01 01 11 01 10 00)	(01 00 10 10 11 10)
(11 00)	(11 11 00 11 11 00)	(11 00 11 11 00 11)
(00 10)	(00 10 10 11 10 01)	(00 10 10 11 10 01)
(00 01)	(00 01 01 11 01 10)	(00 01 01 11 01 10)
(00 11)	(00 11 11 00 11 11)	(00 11 11 00 11 11)
(10 10)	(10 00 01 01 11 01)	(10 10 11 10 01 00)
(01 10)	(01 11 01 10 00 01)	(01 10 00 01 01 11)
(11 10)	(11 01 10 00 01 01)	(11 10 01 00 10 10)
(10 01)	(10 11 10 01 00 10)	(10 01 00 10 10 11)
(01 01)	(01 00 10 10 11 10)	(01 01 11 01 10 00)
(11 01)	(11 10 01 00 10 10)	(11 01 10 00 01 01)
(10 11)	(10 01 00 10 10 11)	(10 11 10 01 00 10)
(01 11)	(01 10 00 01 01 11)	(01 11 01 10 00 01)
(11 11)	(11 00 11 11 00 11)	(11 11 00 11 11 00)

* Autonomous response of LSS.

Table 5.4.2b: (6,2) Systematic Cyclic Code over \mathbb{Z}_2^2 of
Example 5.4.2*.

Systematic cyclic code based on g_o a unit		Systematic cyclic code based on g_r a unit	
\underline{u}	\underline{y}	\underline{u}	\underline{y}
(00 00)	(00 00 00 00 00 00)	(00 00)	(00 00 00 00 00 00)
(10 00)	(10 00 01 01 11 01)	(00 10)	(00 10 01 11 01 01)
(01 00)	(01 00 10 10 11 01)	(00 01)	(00 01 10 11 10 10)
(11 00)	(11 00 11 11 00 11)	(00 11)	(00 11 11 00 11 11)
(00 10)	(00 10 10 11 10 01)	(10 00)	(10 00 01 10 11 10)
(00 01)	(00 01 01 11 01 10)	(01 00)	(01 00 10 01 11 01)
(00 11)	(00 11 11 00 11 11)	(11 00)	(11 00 11 11 00 11)
(10 10)	(10 10 11 10 01 00)	(10 10)	(10 10 00 01 10 11)
(01 10)	(01 10 00 01 01 11)	(10 01)	(10 01 11 10 01 00)
(11 10)	(11 10 01 00 10 10)	(10 11)	(10 11 10 10 00 01)
(10 01)	(10 01 00 10 10 11)	(01 10)	(01 10 11 10 10 00)
(01 01)	(01 01 11 01 10 00)	(01 01)	(01 01 00 10 01 11)
(11 01)	(11 01 10 00 01 01)	(01 11)	(01 11 01 01 00 10)
(10 11)	(10 11 10 01 00 10)	(11 10)	(11 10 10 00 01 10)
(01 11)	(01 11 01 10 00 01)	(11 01)	(11 01 01 00 10 01)
(11 11)	(11 11 00 11 11 00)	(11 11)	(11 11 00 11 11 00)

* $g(x) = 1+x+(1+a)x^2+x^3+ax^4$

codewords of the systematic (6,2) cyclic code based on g_r a unit listed in the fourth column are (0 0 0 0 0 0), (0 a 1 1+a 1 1) (0 1 a 1+a a a), (0 1+a 1+a 0 1+a 1+a).

We note that the set of codewords in the first three cases are same whereas in the last case the codewords are in the reverse order.

5.4.2 Minimum distance Properties

The minimum distance d of a cyclic code over $P_p^n[W(a)]$ generated by a generating polynomial $g(x)$ is the least weight of a codeword in the code. From the result of the Theorem 5.3.4 we have the following.

Theorem 5.4.4 :

An (N,K) linear cyclic code over $P_p^n[W(a)]$, $N \geq 3$ generated by $g(x)$ with g_0 and g_r units has a minimum distance at least 3 if N is the least integer such that $g(x)$ divides (x^N-1) .

Proof :

The proof follows from the result of the Theorem 5.3.4.*

The actual computation of d depends on $g(x)$ and the ring $P_p^n[W(a)]$ over which it is defined. In the following we obtain the minimum distance d of (N,K) cyclic code over semi-local ring $P_p^n[W(a)]$. The approach is similar to the case of cyclic codes over semisimple Z_m given in [48]. We also obtain an expression for minimum distance of a specific case of cyclic codes over semisimple $P_p^n[W(a)]$.

Theorem 5.4.5

Consider a semilocal $P_p^n[W(a)]$, where $W(a) = \prod_{i=1}^v W_i^{h_i}(a)$. Suppose we have (N_i, K) cyclic code over local ring

$P_p^{h_i n_i}[W_i^{h_i}(a)]$, with minimum distance d_i' , $i = 1, 2, \dots, v$.

Then there is a (N, K) cyclic code over semilocal $P_p^n[W(a)]$ with minimum distance $d = \min[d_1, d_2, \dots, d_v]$.

where $N = \text{lcm}(N_1, N_2, \dots, N_v)$

and $d_i = \frac{d_i'}{N_i} N$, $i = 1, 2, \dots, v$.

Proof :

Consider (N_i, K) cyclic code over $P_p^{h_i n_i}[W(a)]$. Since $N = \text{lcm}(N_1, N_2, \dots, N_v)$, N_i divides N . We denote by $C^{(i)}$ the (N, K) cyclic code over $P_p^{h_i n_i}[W_i^{h_i}(a)]$, where each codeword repeats N/N_i times, $i = 1, 2, \dots, v$.

We have seen in Section 2.4 that

$$P_p^n[W(a)] \cong P_p^{h_1 n_1}[W_1^{h_1}(a)] \oplus \dots \oplus P_p^{h_v n_v}[W_v^{h_v}(a)]$$

Consider the external direct sum of codewords, where the components are from $C^{(1)}, C^{(2)}, \dots, C^{(v)}$. The set of all such codewords constitute C

$$C \cong C^{(1)} \oplus C^{(2)} \oplus \dots \oplus C^{(v)}.$$

Then C is a (N, K) cyclic code over $P_p^n[W(a)]$.

A codeword $y = (y_0 \ y_1 \ \dots \ y_{N-1})$ in C has a one to one correspondence with the ν -tuple $y^{(1)}, y^{(2)}, \dots, y^{(\nu)}$.

$$y \approx (y^{(1)}, y^{(2)}, \dots, y^{(\nu)})$$

where $y^{(i)} = (y_0^{(i)} \ y_1^{(i)} \ \dots \ y_{N-1}^{(i)})$

is a codeword of length N in $C^{(i)}$,

$$\text{and } y_j \approx (y_j^{(1)} \ y_j^{(2)} \ \dots \ y_j^{(\nu)}) \quad (5.4.4)$$

The correspondence is established using the Chinese remainder Theorem (Appendix E). For the sake of convenience we represent the ν tuple given in correspondence (5.4.4) as a column vector. Then a codeword in C is

$$y = (y_0 \ y_1 \ \dots \ y_{N-1}) \approx \begin{bmatrix} y_0^{(1)} & y_1^{(1)} & \dots & y_{N-1}^{(1)} \\ y_0^{(2)} & y_1^{(2)} & \dots & y_{N-1}^{(2)} \\ \vdots & \vdots & & \vdots \\ y_0^{(\nu)} & y_1^{(\nu)} & & y_{N-1}^{(\nu)} \end{bmatrix} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \vdots \\ y^{(\nu)} \end{bmatrix}$$

The minimum distance of (N_i, K) cyclic code over $P_p^{h_i n_i} [W_i^{h_i}(a)]$ is d_i' . Therefore, the minimum distance of (N, K) cyclic code $C^{(i)}$ over $P_p^{h_i n_i} [W_i^{h_i}(a)]$ is $d_i = \frac{d_i'}{N_i} N$.

Consider the set of all codewords in C which has the correspondence to the ν -tuples of the form

$$\begin{bmatrix} 0 \\ 0 \\ y^{(i)} \\ 0 \end{bmatrix}$$

where all the external direct sum components except the i th one are zeros. The minimum distance in this set of codewords is equal to the minimum weight of $C^{(i)}$, i.e., d_i . If d is the minimum distance in C a codeword in C can have utmost $(N-d)$ zeros. Since a location in any codeword in C has a zero iff all external direct sum components corresponding to that location are zeros, $d = \text{minimum } [d_1, d_2, \dots, d_v]$. *

Now we consider specific case of cyclic codes over semisimple ring. Since a semisimple ring is a direct sum of Galois fields a cyclic code over semisimple ring is isomorphic to external direct sum of cyclic codes over Galois fields. In the following we consider the direct sum of cyclic codes which are generated as the maximum length sequences over $GF(p^{n_i})$, $i = 1, 2, \dots, v$.

A maximum length sequence over $GF(p^{n_i})$ of length $N_i = (p^{n_i K} - 1)$ can be generated for every p, n_i and K [12]. The set of all cyclic shift of the maximum length sequence and the zero sequence constitutes an (N_i, K) cyclic code $C^{(i)}$ over $GF(p^{n_i})$. $C^{(i)}$ is then called maximum period cyclic code [12]. Since each nonzero codeword is a cyclic shift of the maximum length sequence, the nonzero codewords are all of equal weight. As seen in Section 4.4 the number of zeros in the maximum length sequence is $(p^{n_i(K-1)} - 1)$. Hence the minimum weight of the code $C^{(i)}$ is $d_i = N_i - (p^{n_i(K-1)} - 1)$.

Let $P_p^n[W(a)]$ be a semisimple ring where $W(a) = \prod_{i=1}^v W_i(a)$;

$W_i(a)$ irreducible polynomial of degree n_i over $GF(p)$;

$i = 1, 2, \dots, v$ and (N_i, K) be a maximum period cyclic code over $P_p^{n_i}[W_i(a)]$, $i = 1, 2, \dots, v$. Let $N = \text{lcm}(N_1, N_2, \dots, N_v)$. In the following theorem we obtain an expression for the minimum distance d of the (N, K) cyclic code over semisimple $P_p^n[W(a)]$.

Theorem 5.4.6 :

If $C^{(i)}$ is a maximum period (N_i, K) cyclic code over $P_p^{n_i}[W_i(a)]$ with minimum distance $d_i' = (p^{n_i} - 1) p^{n_i(K-1)}$;
 $i = 1, 2, \dots, v$.

Then $C \cong C^{(1)} \oplus C^{(2)} \oplus \dots \oplus C^{(v)}$ is an (N, K) cyclic code over $P_p^n[W(a)]$ with minimum distance d_1

where $N = \text{lcm}(N_1, N_2, \dots, N_v)$

$$d_1 = \frac{d_1' N}{N_1}$$

and $n_1 \leq n_j$ for all $j = 2, 3, \dots, v$.

Proof : From the result of Theorem 5.4.5 minimum distance d of C is given by minimum $\{d_1, d_2, \dots, d_v\}$.

$$= \text{minimum} \left\{ \frac{d_1'}{N_1} N, \frac{d_2'}{N_2} N, \dots, \frac{d_v'}{N_v} N \right\}$$

$$d_1' = N_1 - (p^{n_1(K-1)} - 1)$$

$$d_1 = \left(1 - \frac{p^{n_1(K-1)} - 1}{N_1}\right) N$$

Hence minimum of d_i occurs for maximum of $(\frac{p^{n_i(K-1)} - 1}{N_i})$

$$i = 1, 2, \dots, \nu$$

We have seen in Section 4.4 that if

$$n_1 \leq n_j \quad \text{for all } j = 2, 3, \dots, \nu$$

$$\begin{aligned} \text{then maximum } \{ \frac{p^{n_1(K-1)} - 1}{N_1}, \dots, \frac{p^{n_\nu(K-1)} - 1}{N_\nu} \} \\ = \frac{p^{n_1(K-1)} - 1}{N_1} \end{aligned}$$

Hence minimum distance $d = d_1$.

*

Example 5.4.3 :

Consider a $(3,2)$ maximum period cyclic code $C^{(1)}$ over $P_2^1[a+1]$, $N_1 = 2^2 - 1 = 3$.

The minimum weight d_1' of the code is $3 - (2^{2-1} - 1) = 2$.

Consider a $(15,2)$ maximum period cyclic code $C^{(2)}$ over $P_2^2[a^2+a+1]$. $N_2 = [(2^2)^2 - 1] = 15$. The minimum weight d_2' of the code is $= 15 - (2^2 - 1) = 12$.

$$N = \text{lcm}(3, 15) = 15, K = 2.$$

$$\text{Let } C \simeq C^{(1)} \oplus C^{(2)},$$

Then C is a $(15,2)$ code over $P_2^3[a^3+1]$.

The minimum weight of the code is

$$d = \frac{d_1}{N_1} \cdot N = \frac{2}{3} \times 15 = 10.$$

5.4.3 Decoding Principles

Cyclic codes over $P_p^n[W(a)]$ being specific case of polynomial codes, the decoding procedure of polynomial codes by syndrome computation discussed in Section 5.3 can be used. Just as in the case of polynomial codes, the encoder implementation must be known for syndrome computation. Because of the additional structure of cyclic codes, two more methods of decoding can be used; (i) Hamming cross-correlation method (ii) Permutation decoding. Hamming cross-correlation method can be used to decode systematic or nonsystematic cyclic codes and is based on the Hamming cross correlation value of the code sequences. Permutation decoding can be used to decode systematic cyclic codes; the principle is similar to the one used for decoding systematic cyclic codes over finite fields proposed in [54]. In both these methods the knowledge of the encoder implementation is needed at the decoder. In the Hamming cross-correlation method the encoder decides the sense of cyclic shift for computing the cross-correlation values and in permutation decoding identical encoders are used for generating the codewords at the receiver. Encoder implementation must also be known for recovering the message from the corrected version of the received word.

(I) Permutation Decoding :

Permutation decoding is based on the symmetry of the code where a permutation of the symbol positions of a codeword is also a codeword. If the same permutation is applied to the symbols of every codeword and if each codeword is changed, it is changed into another codeword in the code. Permutation decoding is useful for systematic codes with high redundancy and hence with high error correcting capabilities [54].

Let us consider an (N, K) systematic cyclic codes, where the first K symbols are the message symbols. The other $(N-K)$ symbols are the check symbols. For a given message word u of length K we have the encoded word which we represent by $E(\underline{u})$. Let \bar{y} stand for the first K symbols of a word y of length N . y is a codeword iff

$$y = E(\bar{y}) \quad (5.4.5)$$

Let π be the cyclic permutation (cyclic shift) of symbol positions in the set of all N -tuples over $P_p^n[W(a)]$. If y is a codeword then πy is also a codeword. The first K positions of πy are information symbols and

$$\pi y = E(\overline{\pi y}) \quad (5.4.6)$$

Let y' be a received word containing $\leq e$ errors. If no errors have occurred in the first K places of y' , then $y = E(\overline{y'})$ is the unique word of the code at distance $\leq e$ from y' . On the

other hand if one or more errors have occurred in the first K places of y' the word $E(\bar{y}')$ is not the corrected version of y' since $E(\bar{y}')$ is the same as y' in the first K places. In this case $E[\bar{y}']$ is at a distance $> e$ from y' .

The decoding procedure is as follows :

Form $y = E(\bar{y}')$ and find distance between y' and y . If the distance is $\leq e$, y is the correct version of y' .

Let y denotes the unique codeword at a distance $\leq e$ from y' . The distance between πy and $\pi y'$ is the same as that of y and y' .

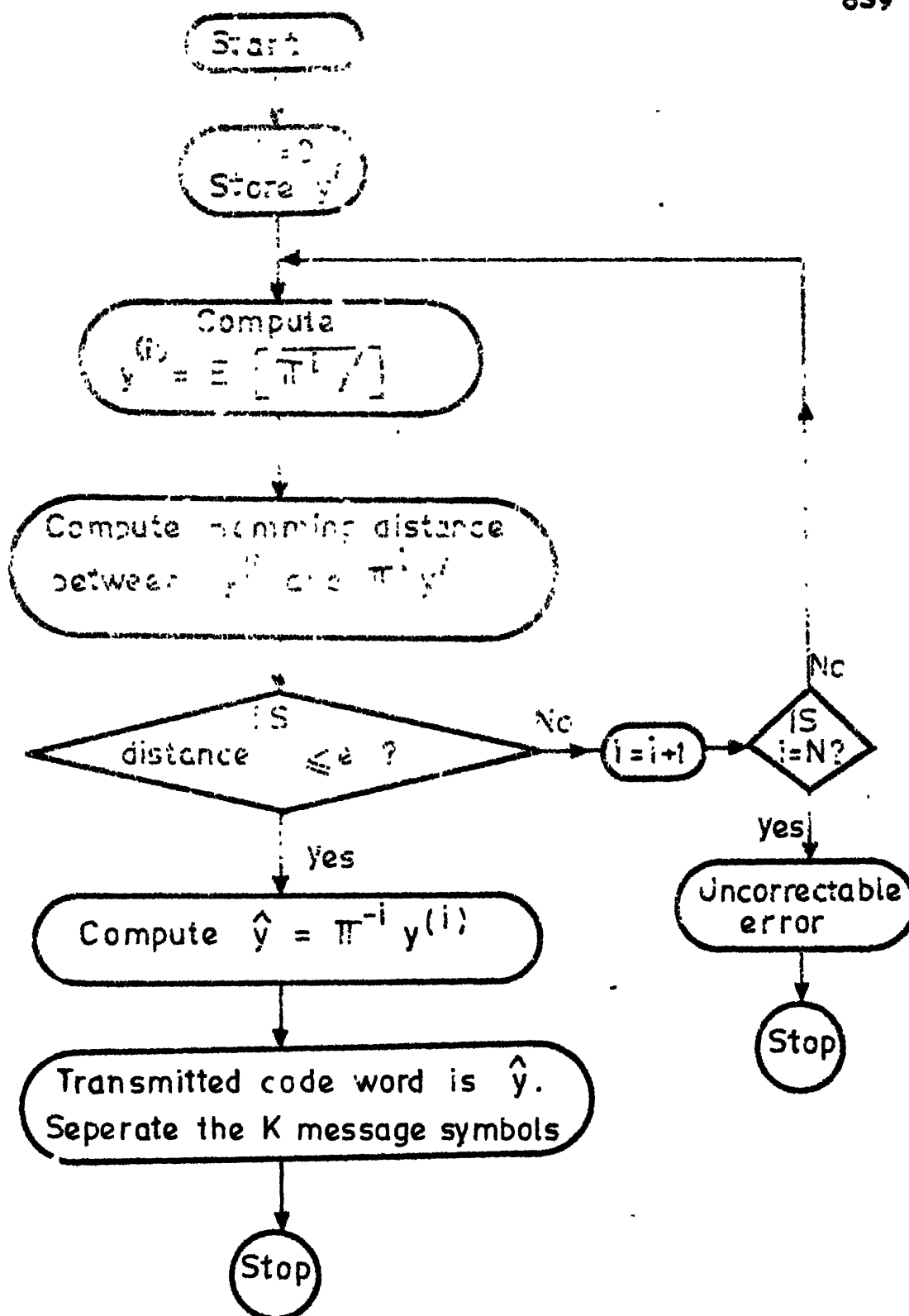
Suppose π^i is a cyclic shift which moves the error in y' out of the first K positions. Then $y^{(i)} = E(\pi^i \bar{y}')$ is at a distance $\leq e$ from $\pi^i y'$ and is the unique codeword in the code with this property. Consequently $\hat{y} = \pi^{-i} y^{(i)}$ is the corrected version of y' .

The decoding procedure is given in the Flow Chart 5.4.1.

For the decoding of the codeword, the first K symbols in the shifted version of received word must be error free, that is, there must be a gap of at least K symbols between two error locations.

Example 5.4.4

Consider a $(6,2)$ systematic cyclic code generated by the following LSS over $P_2^2[a^2+1]$ of Example 5.4.2. The feedback



Flow Chart 5.4.1 Procedure for Permutation Decoding

polynomial of the LSS is $(1+x+ax^2)$ and the LSS is given in Figure 5.4.1. The codewords are tabulated in Table 5.4.1a.

The first 2 symbols are the message symbols. The minimum weight of the code is 4. Hence can correct single errors.

Let the message word u be $= (a \ a)$

Then the codeword is $y = (a \ a \ 1+a \ a \ 1 \ 0)$

Let the error word be $e = (1+a \ 0 \ 0, 0, 0, 0)$

Then the received word $y' = (1 \ a \ 1+a, a, 1, 0)$

We note from the Table 5.4.3 that for $i = 1$ the distance between $y^{(i)}$ and $\pi^i y'$ is 1. Hence, corrected codeword is $\pi^{-1} y^{(i)} = (a, a, 1+a \ a \ 1 \ 0)$.

The codewords over $\mathbb{Z}_2^2 \cong \mathbb{P}_2^2[a^2+1]$ are

$(10 \ 00 \ 01 \ 01 \ 11 \ 01)$

$(00 \ 10 \ 10 \ 11 \ 10 \ 01)$

$(00 \ 11 \ 11 \ 00 \ 11 \ 11)$

and their cyclic shifts.

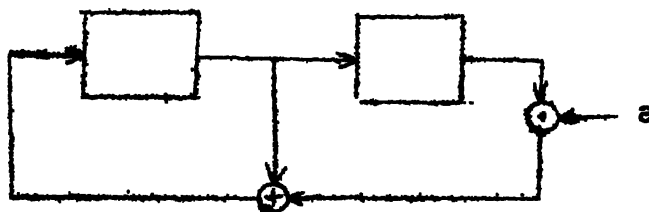


Figure 5.4.1 LSS of Example 5.4.4

The received word in this example in terms of 2-tuples over \mathbb{Z}_2^2 is (10 01 11 01 10 00) and the decoded codeword is (01 01 11 01 10 00).

(II) Decoding by Hamming Cross Correlation

We have seen in Section 4.2 that if the cycle length decomposition of a nonsingular $P_p^n[W(a)]$ -LSS is $[\mu_1(c_1) \mu_2(c_2), \dots, \mu_r(c_r)]$, then there are $\mu = \sum_{i=1}^r \mu_i$ output sequences distinct upto cyclic shifts. The total number of sequences is p^n . Suppose the cyclic code is generated as an autonomous response of nonsingular single output canonical LSS. Then the codeword is one of the μ sequences of length N or its cyclic shifts. The Hamming correlation property of such sequences is made use of in the decoding. This method need not be restricted to cyclic codes generated as the autonomous response of LSS. Since in a cyclic code every codeword is a multiple of $g(x)$, the method applies equally well to cyclic codes generated as the forced response of LSS also. The distinct codewords upto cyclic shifts, the minimum distance and the encoder used are to be known. In Section 4.4 the procedure for the computation of maximum Hamming auto-correlation function value for $\tau \neq 0$ or maximum Hamming cross-correlation value of sequences over semisimple ring with projection of $f(x)$ over $P_p^{n_i}[W_i(a)]$ being primitive $i = 1, 2, \dots, v$ is given. If the maximum value of Hamming cross-correlation function between pairs of two sequences in the set is δ_m then $N - \delta_m$ is the minimum distance of the code.

At the receiver we have μ distinct reference sequences of length N which are codewords. In the absence of noise the received word is one of these sequences with or without cyclic shifts. The received word is cross-correlated with all the μ reference sequences. The decoder performs the following two tasks :

- (i) finds the correlator whose output has a peak value N ; then the received word is a cyclic shift of the reference word of that correlator.
- (ii) finds the location of the peak value; if the received word is the reference word itself the peak occurs at shift $\tau = 0$; if it is a cyclic shift of reference word the peak occurs at τ , corresponding to the cyclic shift. Thus by knowing the location at which peak occurs the received word is determined.

In the presence of noise the situation is different. Some symbols of the received word are altered by the noise. However, as we see below, if the number of errors is within the error correcting capability, it is possible to decode.

We have seen in Section 4.4, that in the set of autonomous responses of length N of a nonsingular, canonical single output $p_p^n[W(a)]$ -LSS for $\tau \neq 0$, the maximum value of HACR function of any sequence and maximum value of HCCR function between any two sequences is given by $\max \{ \delta_1, \delta_2, \dots, \delta_\mu \}$ where δ_i is

the number of zeros in the i th distinct sequence. $i = 1, 2, \dots, \mu$. Let $\max \{\delta_1 \ \delta_2 \ \dots \ \delta_\mu\}$ be δ_m . This implies that the Hamming cross-correlation function value between any two sequences of length N in the set is less than or equal to δ_m and Hamming autocorrelation function value of any sequence in the set for $\tau \neq 0$ is $\leq \delta_m$.

Typical HCCR and HACR functions are given in Figures 5.4.2a, b and c.

If the correlation is between a sequence and its cyclic shifted version shifted by τ' positions, then the correlation function is as shown in Figure 5.4.2c.

Let y be the received word in which e' number of symbol errors have occurred. Then the corresponding correlator outputs in the μ correlators is one of the form given in Figure 5.4.3a, b and c.

The effect of e' symbols being altered in y is to decrease the peak value of HACR function from N to at most $N - e'$ and increase the values for $\tau \neq 0$ from δ_m to at most $\delta_m + e'$.

Likewise the HCCR function values are increased from δ_m to at most $\delta_m + e'$. That is the effect of error is to alter the values by at most e' units.

A peak value can be detected without ambiguity as long as

$$(N - e') \geq (\delta_m + e') + 1 .$$

$$(N - \delta_m) \geq (2e' + 1) .$$

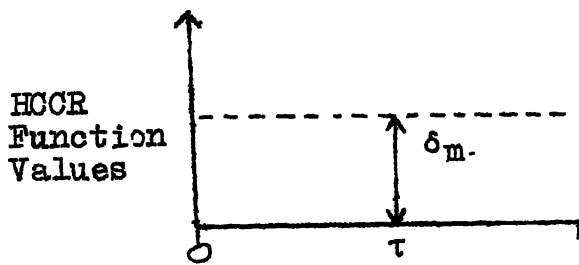


Figure 5.4.2a HCCR function values
 $\leq \delta_m$

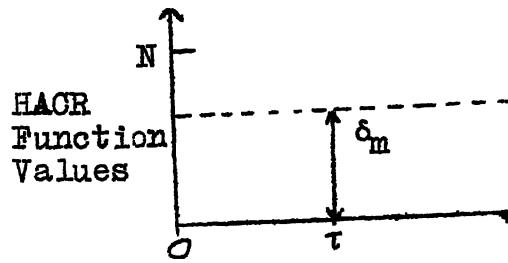


Figure 5.4.2b HACR function values N
for $\tau = 0$ and $\leq \delta_m$, $\tau \neq 0$

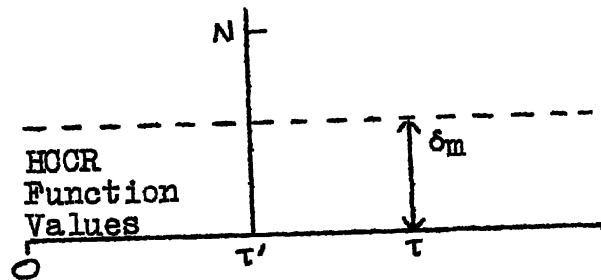


Figure 5.4.2c HCCR function values :
 N for $\tau = \tau'$ and $\leq \delta_m$ for $\tau \neq \tau'$

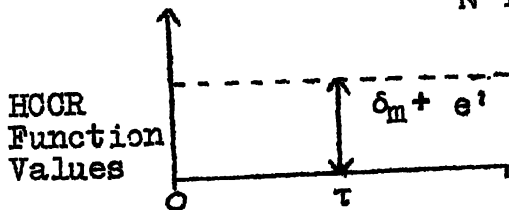


Figure 5.4.3a HCCR function values
 $\leq \delta_m + e'$

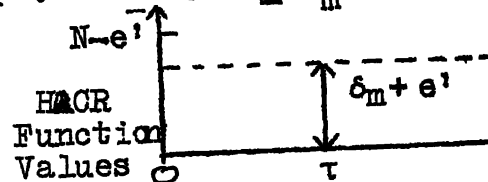


Figure 5.4.3b HACR function
values $N - e'$ for $\tau = 0$
and $\leq \delta_m + e'$ for $\tau \neq 0$

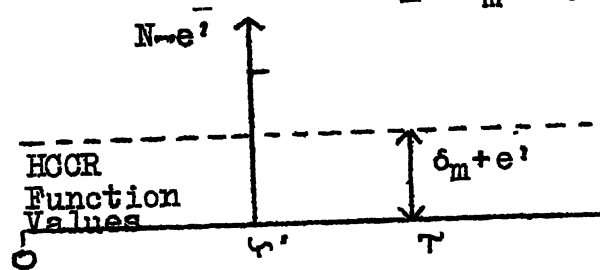


Figure 5.4.3c HCCR function values $N - e'$ for $\tau = \tau'$
and $\delta_m + e'$ for $\tau \neq \tau'$

This implies that as long as the error is within the error correcting capability, the peak is detected and hence the transmitted codeword is determined.

Decoding procedure is given in the Flow chart 5.4.2. y' is the received word and $y_{(1)}, y_{(2)} \dots y_{(\mu)}$ are the local reference codewords. $\sigma y_{(i)}$ is the cyclic shift of i th reference word.

Example 5.4.5

We consider the $(6,2)$ cyclic code over $P_2^2[a^2+1]$ of Example 5.4.2 which are listed in Table 5.4.1a. The codewords are

$$y_{(0)} = (0 \ 0 \ 0 \ 0 \ 0 \ 0)$$

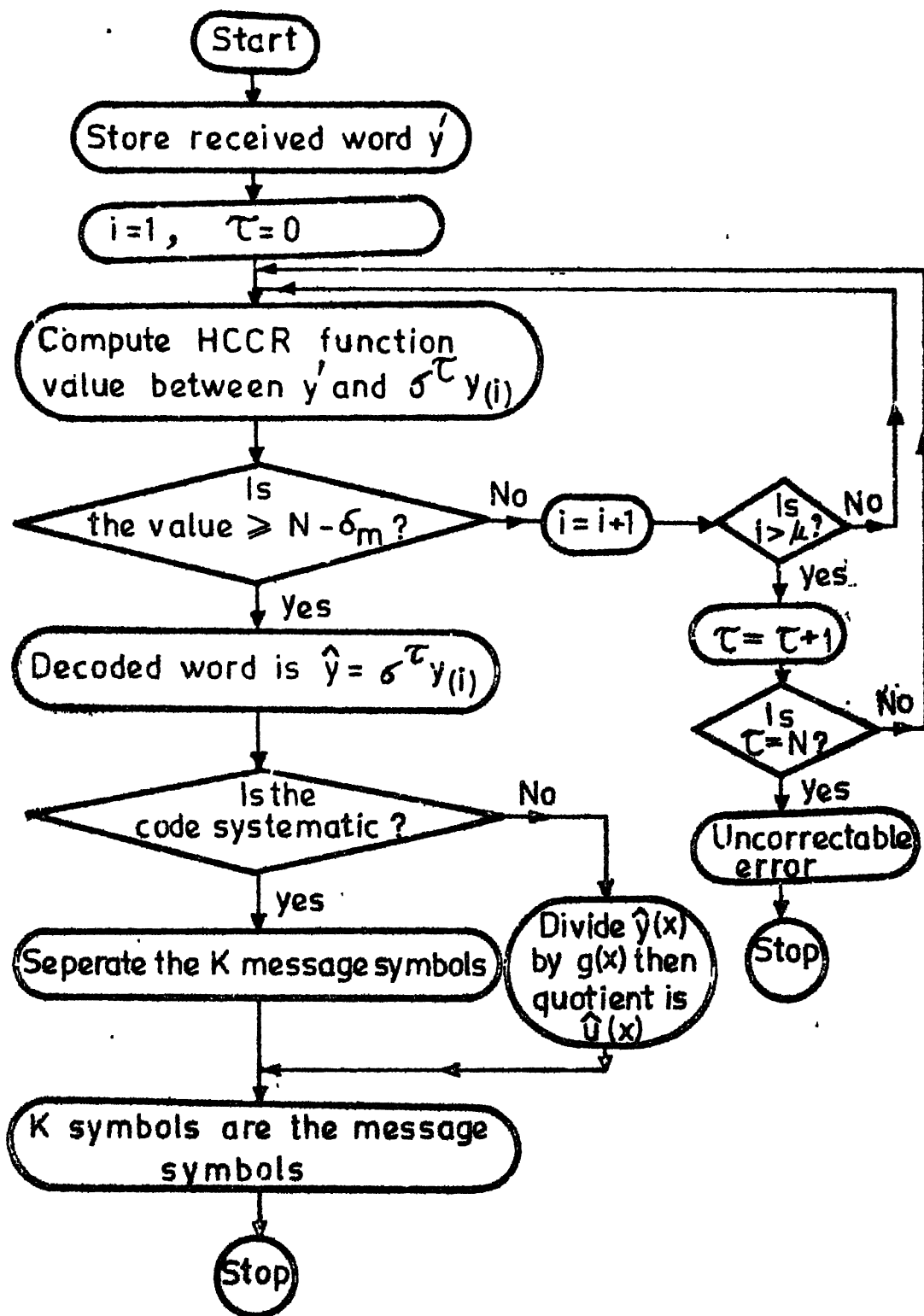
$$y_{(1)} = (1 \ 0 \ a \ a \ 1+a \ a)$$

$$y_{(2)} = (a \ 0 \ 1 \ 1 \ 1+a \ 1)$$

$$y_{(3)} = (1+a \ 0 \ 1+a \ 1+a \ 0 \ 1+a)$$

and their cyclic shifts. Hence the code has $\mu = 4$ distinct codewords $y_{(0)}, y_{(1)}, y_{(2)}$ and $y_{(3)}$ upto cyclic shifts. The minimum distance of the code is 4 and hence the maximum value of HCCR function between any two sequences is $\delta_{la} = 2$. The code can therefore correct single errors.

Suppose the received word is $y' = (a \ a \ 0 \ a \ 1 \ 0)$. The decoding procedure given in Flow Chart 5.4.2 is used for



Flow Chart.5.4.2 Procedure for Hamming Cross-correlation Decoding

decoding the received word y' . The Hamming cross correlation function values between the received word and the reference words $y_{(0)}$, $y_{(1)}$, $y_{(2)}$ and $y_{(3)}$ for shifts $\tau = 0, 1, 2, 3, \dots$ are computed. These values are tabulated in Table 5.4.4.

Decoding is based on the reference word for which the HCCR function value is greater than $(N - \delta_m) = (6 - 2)$ and the associated shift. From the Table 5.4.4 we see that for $\tau = 4$ the HCCR function value between y' and $y_{(1)}$ is $5 > (6 - 2)$. Hence the corrected codeword is $\sigma^4 y_{(1)} = (a \ a \ (1+a) \ a \ 1 \ 0)$. By knowing the encoder implementation, the message symbols can be recovered from the corrected word.

Table 5.4.4 HCCR function values between y' and $y_{(0)}$, $y_{(1)}$, $y_{(2)}$ and $y_{(3)}$

τ	$H_{y', y_{(0)}}(\tau)$	$H_{y', y_{(1)}}(\tau)$	$H_{y', y_{(2)}}(\tau)$	$H_{y', y_{(3)}}(\tau)$
0	2	1	1	0
1	2	3	3	2
2	2	1	1	1
3	2	1	1	1
4	2	5	1	2
5	2	1	1	0

5.5 ENCODERS FOR POLYNOMIAL AND CYCLIC CODES OVER $P_p^n[W(a)]$

In this section we give three basic encoder structures for polynomial and cyclic codes over $P_p^n[W(a)]$. As we shall see these structures are inherently $P_p^n[W(a)]$ -LSS of appropriate order. Encoder No.1 generates nonsystematic polynomial and cyclic codes. Encoder No.2 generates systematic polynomial and cyclic codes. Encoder No.3 generates systematic cyclic codes. Encoders for interleaved polynomial and cyclic codes for burst error correction are also given. In all of these encoder structures various operations concerning the ring elements are implemented in a parallel fashion. However, when $W(a) = (a^n - 1)$ serial encoder structures based on serial implementation of $P_p^n[W(a)]$ -LSS as discussed in Section 3.5 are possible; details of these are included.

Consider an (N, K) polynomial or cyclic code with message and codeword polynomials,

$$u(x) = u_0 + u_1x + \dots + u_{K-2}x^{K-2} + u_{K-1}x^{K-1} \quad \text{and}$$

$$y(x) = y_0 + y_1x + \dots + y_{N-2}x^{N-2} + y_{N-1}x^{N-1} \quad \text{respectively.}$$

In what follows, for the sake of convenience we call the symbols u_0, y_0 as least degree symbols and u_{K-1}, y_{N-1} as the highest degree symbols.

5.5.1 Basic Encoder Structures

We take up the details of Encoders No.1, No.2 and No.3.

Structures of these encoders are analogous to encoders for codes over finite fields given in [12,17-21] we call these structures basic encoder structures as they constitute the core for the interleaved encoders discussed in the next subsection.

Encoder No.1

We have seen in Sections 5.3 and 5.4 that in an (N,K) polynomial or cyclic code over $P_p^n[W(a)]$, every codeword polynomial $y(x)$ is a product of generating polynomial $g(x) = g_0 + g_1x + \dots + g_rx^r$ and the message polynomial $u(x)$. A $(N-K)$ th order feed forward $P_p^n[W(a)]$ -LSS, called Encoder No.1 can be employed to perform the multiplication of $u(x)$ by $g(x)$. Two cases are possible depending on the order in which the feedforward coefficients g_0, g_1, \dots, g_r are arranged

Case (i) ; Feedforward coefficients are arranged as $(g_0g_1 \dots g_r)$ and the lowest degree symbol of $u(x)$ enters the encoder first. The encoder structure is shown schematically in Figure 5.5.1a. The characterising matrices of the LSS are

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & \vdots & \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} ; \quad B = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} ; \quad C = [g_r, g_{r-1}, \dots, g_1] ;$$

$$D = [g_0] .$$

The encoding operation is as follows. Initially the state of the LSS is zero. The input of message symbols $u_0, u_1 \dots u_{K-1}$ is given at the commencement of the encoding operation.

The corresponding encoded symbols y_0, y_1, \dots, y_{K-1} appear at the output. A sequence of $(N-K)$ zeros is applied after the K message symbols, and the corresponding sequence (y_K, \dots, y_{N-1}) of output symbols appears at the output. The output sequence $(y_0, y_1, \dots, y_{N-1})$ is the sequence of coefficients of $y(x) = u(x) \cdot g(x)$. The encoding of $u(x)$ being complete the LSS stages are cleared (forced to zero state). The encoder is now ready to accept the next message word. The output sequence symbols given by $y_i = \sum_{j=0}^i g_j u_{i-j}$, $i = 0, 1 \dots (N-1)$. Constitute the forced response of the system with initial state equal to zero. The code generated is in nonsystematic form.

Case (ii) ; Feedforward coefficients are arranged as $g_r, g_{r-1}, \dots, g_1, g_0$ and the highest degree symbol of $u(x)$ enter the encoder first.

The encoder structure is shown schematically in Figure 5.5.1b and is identical to the case i) except for the arrangement of feedforward coefficients. The characterising matrices A and B of the LSS are as for case i). However, $C = [g_0 \ g_1 \ \dots \ g_{r-1}]$ and $D = [g_r]$. The encoding operation is similar to case (i). The input sequence is $(u_{K-1} \ u_{K-2} \ \dots \ u_0 \ 0 \ 0)$ and output is $(y_{N-1} \ y_{N-2} \ \dots \ y_1 y_0)$.

As seen in Section 2.5 there is a one-to-one correspondence between elements of $P_p^n[W(a)]$ and n -tuples over $GF(p)$ of $Z_p^n[W]$. Hence the multiplication of elements in $P_p^n[W(a)]$ can be achieved in terms of the multiplication of an appropriate $n \times n$ matrix and n -vector over $GF(p)$. The Encoder No.1 shown in Figure 5.5.1a and b can hence be implemented over $GF(p)$ where each memory device is replaced by an n -stage shift register which store n -tuples over $GF(p)$ and the scalars $g_0, g_1, \dots, g_r \in P_p^n[W(a)]$ are replaced by appropriate multipliers and adders over $GF(p)$. The multiplication and addition operations of the ring elements are implemented in a parallel fashion and the input and output sequences are n -tuples over $GF(p)$.

Example 5.5.1

Consider the $(4,2)$ polynomial code over $P_2^2[a^2+1]$ given in Example 5.3.5. The generator polynomial of this code is $g(x) = a + (1+a)x + ax^2$. Using the one-to-one correspondence between the elements of $P_2^2[a^2+1]$, the ring of n -tuples Z_p^n and ring of $n \times n$ commutative matrices M_p^n we have, $0 \cong \begin{bmatrix} 0 \\ 0 \end{bmatrix} \cong \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$$a \cong \begin{bmatrix} 0 \\ 1 \end{bmatrix} \cong \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad (1+a) \cong \begin{bmatrix} 1 \\ 1 \end{bmatrix} \cong \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}; \quad 1 \cong \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The Encoder No.1 for this code over $P_2^2[a^2+1]$ corresponding to case 1) is given in Figure 5.5.2a and the encoder over $Z_2^2 \cong P_2^2[a^2+1]$ is given in Figure 5.5.2b. The lowest degree

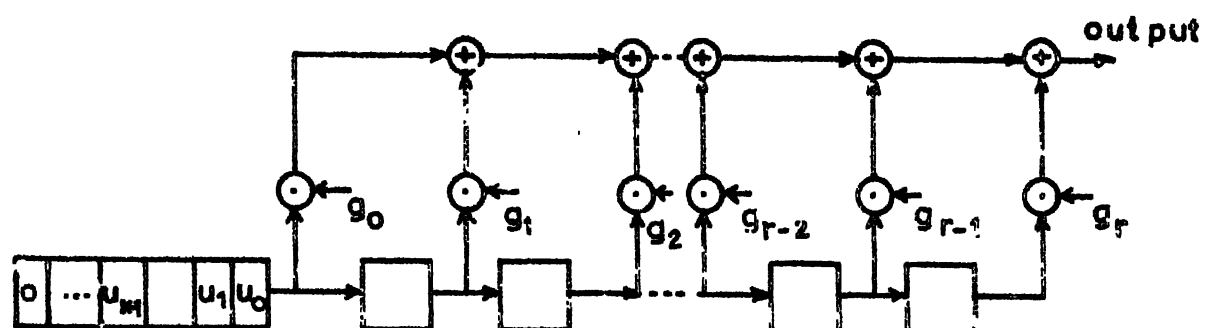


Fig.5.5.1a Encoder No.1 Case (i)

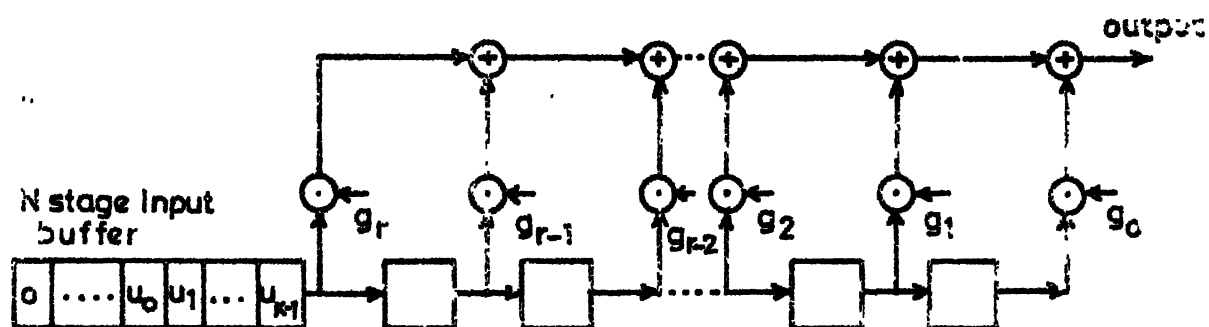


Fig.5.5.1b Encoder No.1 Case (ii)

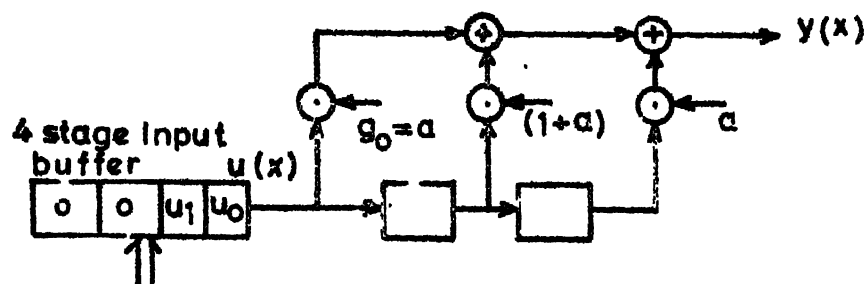


Fig. 5.5.2 a Encoder No.1 over $P_2^2[d^2+1]$
of Example 5.5.1

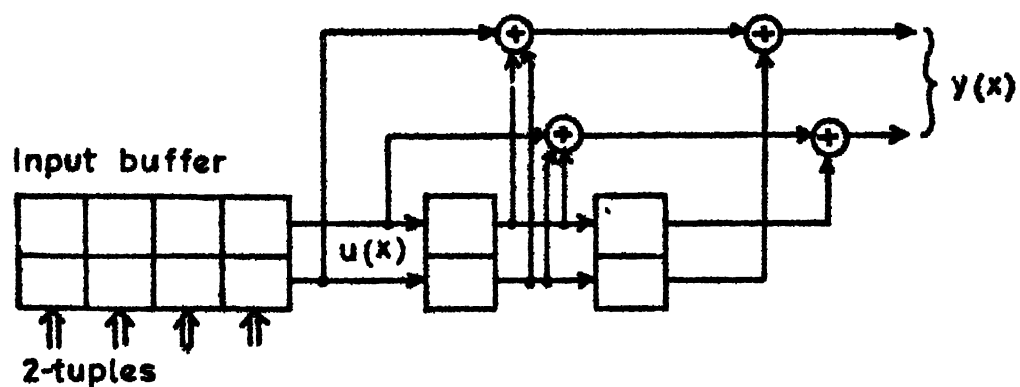


Fig. 5.5.2 b Encoder No.1 over $Z_2^2 \approx P_2^2[d^2+1]$
of Example 5.5.1

symbols are the first input symbol and output symbol respectively. These inputs correspond to scheme given in Figure 5.5.1a.

Encoder No.2

Encoder No.2 generates systematic polynomial or cyclic codes. The principle of Encoder No.2 is based on polynomial division and is discussed in Section 5.3. We have seen in Sections 5.3 and 5.4 that in order for $g(x)$ to be the generator polynomial of a polynomial code it is sufficient that either g_r or g_0 is a unit, while for cyclic codes both g_0 and g_r must be units. Two encoders are given below these are based on (i) g_r a unit with highest degree message symbol entering first and (ii) g_0 a unit with lowest degree message symbol entering first.

Encoder No.2 based on g_r a unit : The encoder performs the following operations. (i) multiplication of the message polynomial $u(x)$ by x^{N-K} , (ii) division of $x^{N-K} u(x)$ by $g(x)$ to get the remainder $R(x)$ whose coefficients are the check symbols and (iii) the formation of codeword polynomial $x^{N-K} u(x) - R(x)$. These operations can be implemented by using a. $(N-K)$ th order feedback $P_p^n[W(a)]$ -LSS shown in Figure 5.5.3. The feedback coefficients g_0, g_1, \dots, g_r are the coefficients of the generating polynomial $g(x)$.

With Gate 1 turned on and Gate 2 turned off the K message symbols $u_{K-1} u_{K-2} \dots u_2 u_1 u_0$ are applied to the $P_p^n[W(a)]$ -LSS and simultaneously to the channel. We note here that the

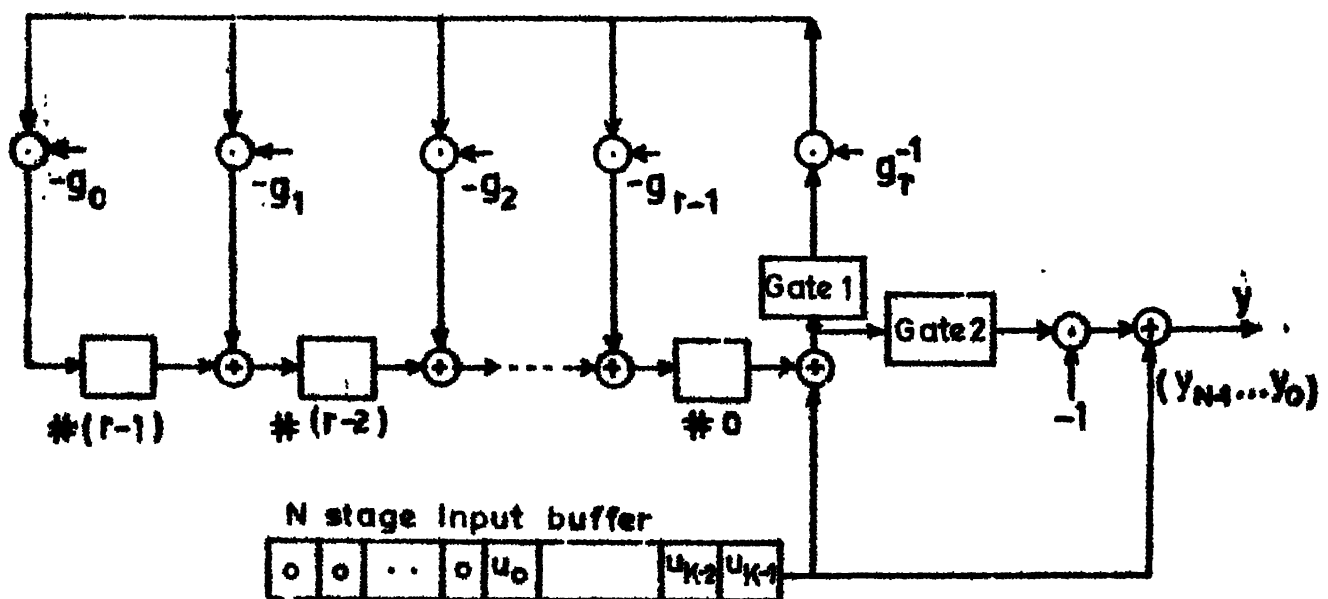


Fig.5.5.3 Encoder No.2 Based on g_r a unit

message symbol sequences are applied with highest degree symbol of $u(x)$ entering first. Applying the message symbol from the right hand side as shown in Figure 5.5.3 is equivalent to pre-multiplying $u(x)$ by x^{N-K} . As soon as the K -message symbols enter the LSS, the $(N-K)$ symbols which are stored in the shift register of LSS constitute the coefficients of the remainder $R(x)$ which are the parity check symbols. The feedback connection now is broken by turning Gate 1 off. Gate 2 is then turned on and the parity check symbols are shifted to the channel. The sequence of output symbols is a sequence of coefficients in the descending powers of x in the codeword polynomial $y(x)$. We note here that the coefficient g_r of $g(x)$ must be a unit in $P_p^n[W(a)]$.

Encoder No.2 based on g_0 a unit : This is based on the principle discussed in Section 5.3. With g_0 of $g(x)$ a unit in $P_p^n[W(a)]$, $u(x)$ is divided by $g(x)$ such that the quotient $q^{(i)}(x)$ and remainder $R^{(i)}(x)$ at the i th step of division are in increasing powers of x . The division is performed upto K steps. The remainder $R^K(x)$ is an r -tuple with least degree of x greater than or equal to K and highest degree of x less than or equal to $(N-1)$. The coefficients of $R^K(x)$ are the parity check symbols. The division is performed in a division circuit using $P_p^n[W(a)]$ -LSS. The scheme is given in Figure 5.5.4 in which it is assumed that $r < K$. The operation is as follows.

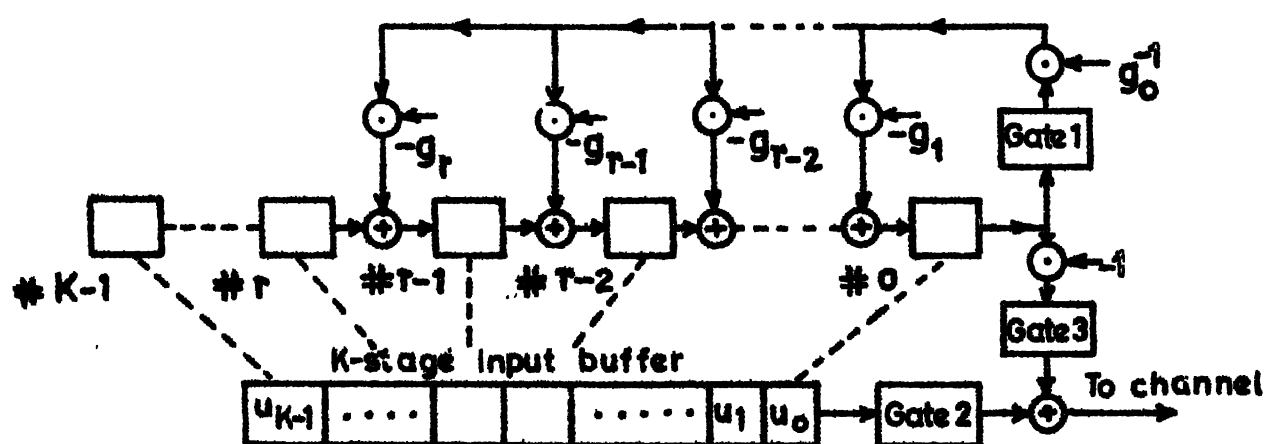


Fig. 5.5.4 Encoder No.2 Based on g_o a unit

At the commencement of the encoding the K message symbols are loaded into the memory devices of a $P_p^n[W(a)]$ -LSS of order K . With Gates 1 and 2 turned on and Gate 3 turned off the contents of the buffer is shifted into the channel, simultaneously the LSS is shifted. At the end of K shifts all the K message symbols are presented to the channel and LSS would have completed the division operation with the coefficient of the remainder stored in the memory devices. Now Gates 1 and 2 are turned off and Gate 3 is turned on. The r parity check symbols are then shifted to the channel after negation. If $r > K$ the $(r-K)$ memory devices in the LSS must be cleared to zero while the remaining devices are loaded with message symbols. The order of the system in this case is either r or K whichever is larger.

The encoders given in Figures 5.5.3 and 5.5.4 can be implemented over $GF(p)$ using the isomorphism $Z_p^n[W] \cong P_p^n[W(a)]$. The input and output sequences are now sequences of n -tuples over $GF(p)$. Each memory device is replaced by an n -stage shift register over $GF(p)$ and the multiplication by each of the coefficients g_0, g_1, \dots, g_r is implemented by using scalars over $GF(p)$ and modulo p adders.

Example 5.5.2

Consider the systematic $(4,2)$ polynomial code over $P_2^2[a^2+1]$ of Example 5.5.1. Encoder No.2 for this code over $P_2^2[a^2+1]$ based on g_r a unit is given in Figure 5.5.5a and over Z_2^2 in Figure 5.5.5b.

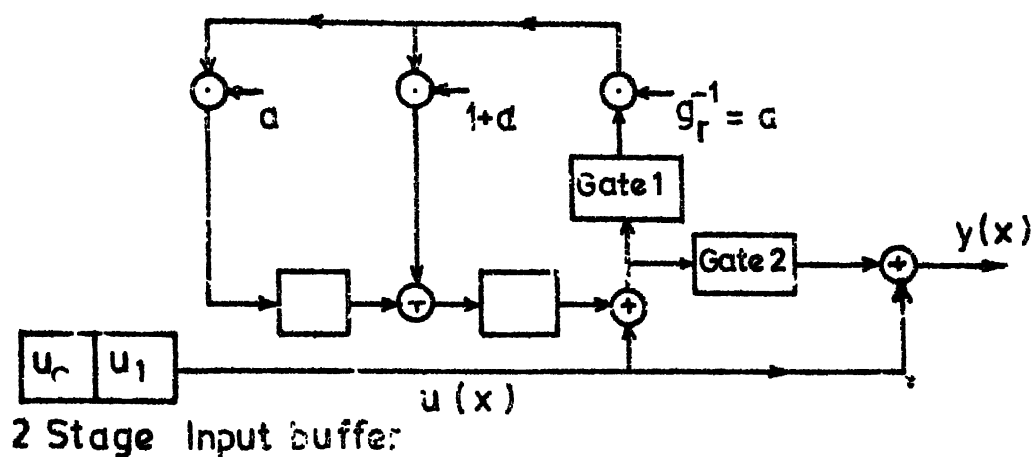


Fig.5.5.5 a Encoder No.2 over $P_2^2 [a^2+1]$ of Example 5.5-2

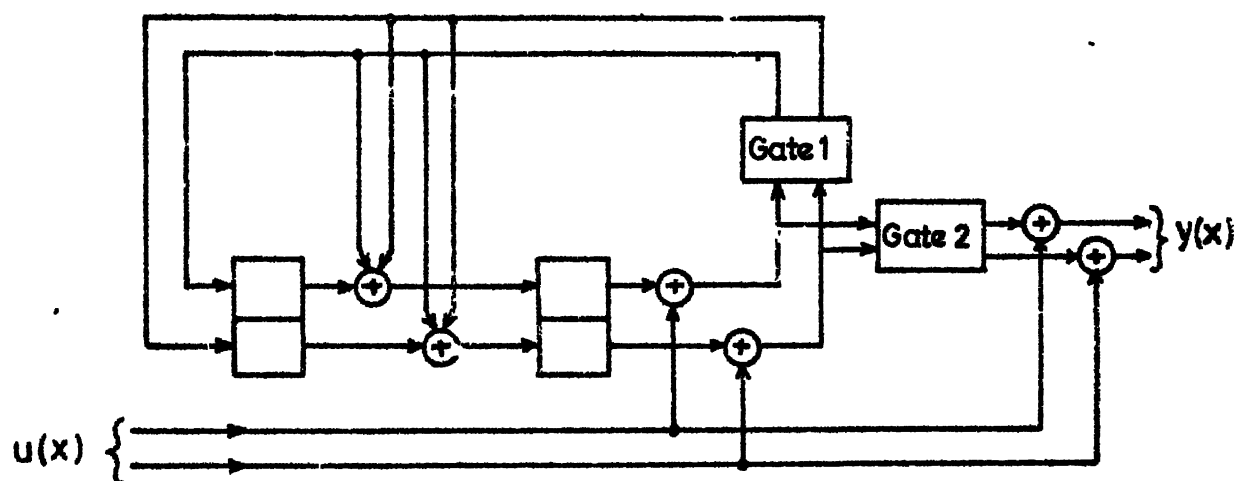


Fig.5.5.5b Encoder No.2 over $Z_2^2 \approx P_2^2 [a^2+1]$ of Example 5.5-2

Note that since $a = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $a^{-1} = a$, multiplication by a or a^{-1} is just the rotation of the 2-tuples.

Example 5.5.3

Consider the (5,3) systematic polynomial code over $P_2^2[a^2+1]$ generated by $g(x) = a+ax+(1+a)x^2$. Encoder No.2 for this code over $P_2^2[a^2+1]$ based on g_0 a unit is given in Figure 5.5.6a and over $Z_2^2 \simeq P_2^2[a^2+1]$ in Figure 5.5.6b.

Encoder No.3

*

In Section 5.4 we have seen that the set of all autonomous responses of length N of LSS of order K constitutes a systematic (N,K) cyclic code. The initial values are the message symbols and N is a multiple of T , the period of characteristic matrix A of the LSS. Let $g(x)$ of degree $r=(N-K)$ be the generating polynomial of the (N,K) cyclic code. Then as seen in Section 5.4 there exists a check polynomial $h(x)$ such that

$$h(x) = \frac{(1-x^N)}{g(x)} = h_0 - \sum_{i=1}^K h_i x^i \quad (5.5.1)$$

Comparing Equation (5.5.1) with Equation (4.3.9) we see that $h(x)$ is the feedback polynomial of a canonical LSS. Hence a nonsingular canonical single output LSS can be used for generating an (N,K) systematic cyclic code. The resulting structure is called Encoder No.3 and is shown in Figure 5.5.7.

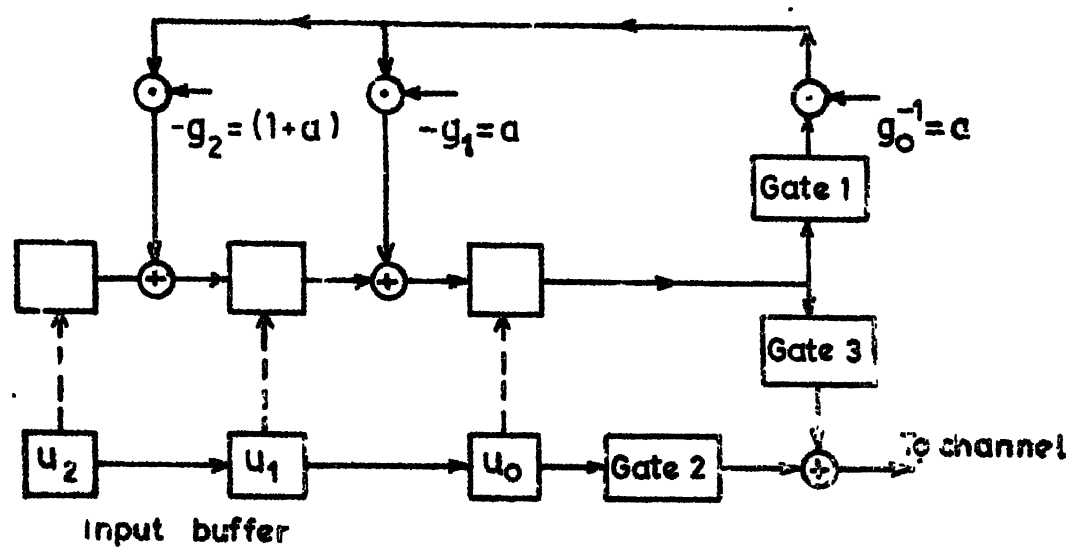


Fig. 5.5.6a Encoder No. 2 over $\mathbb{P}_2^2 [d^2+1]$ of Example 5.5.3

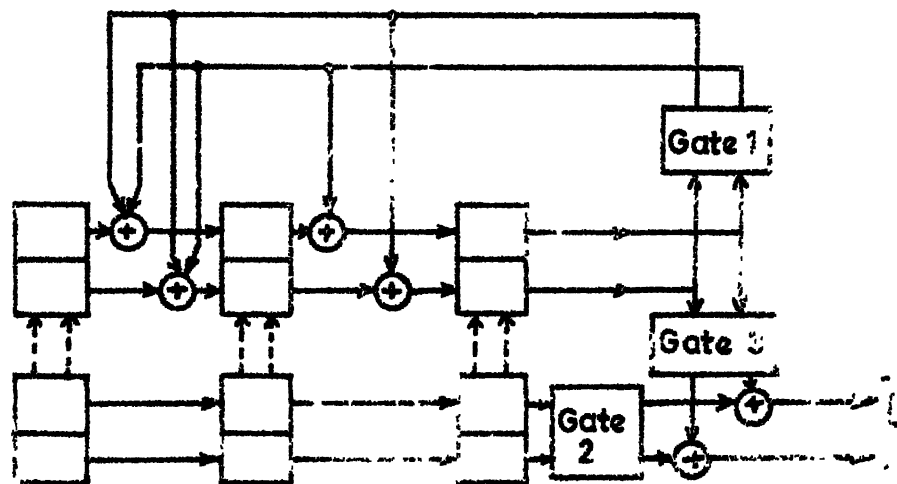


Fig. 5.5.6b Encoder No. 3 over $\mathbb{Z}_2^2 = \mathbb{P}_2^2 [d^2+1]$ of Example 5.5.3

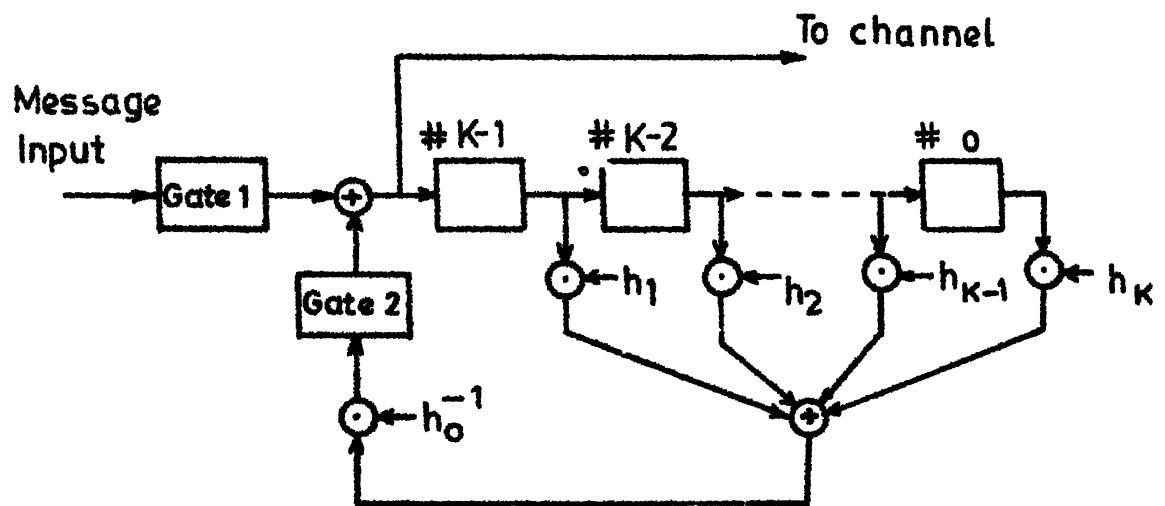


Fig. 5.5.7 Encoder No. 3

The operation is as follows. At the commencement of encoding Gate 1 is turned on and Gate 2 is turned off. The K message symbols are shifted into the LSS with lowest degree symbol entering first and presented to the channel simultaneously. After the K initial values are loaded into the LSS, Gate 1 is turned off and Gate 2 is turned on. During the next $(N-K)$ clock pulses the $(N-K)$ check symbols are formed and presented to the channel. At the end of N th clock pulse Gate 1 is turned on and Gate 2 is turned off. Next message symbol is then encoded as above. The code generated is systematic.

As in the case of Encoders Nos. 1 and 2 the isomorphism between $P_p^n[W(a)]$ and $Z_p^n[W]$ can be utilised to implement Encoder No.3 over $GF(p)$.

Example 5.5.4

Consider the $(6,2)$ cyclic code of Example 5.4.2 generated by $g(x) = 1+x+(1+a)x^2+x^3+ax^4$ over $P_2^2[a^2+1]$. Encoder No.3 for this code is given in Figure 5.5.8a. The feedback polynomial $h(x) = \frac{1-x^6}{g(x)} = 1+x+ax^2$. The encoder over $Z_2^2 \cong P_2^2[a^2+1]$ is given in Figure 5.5.8b.

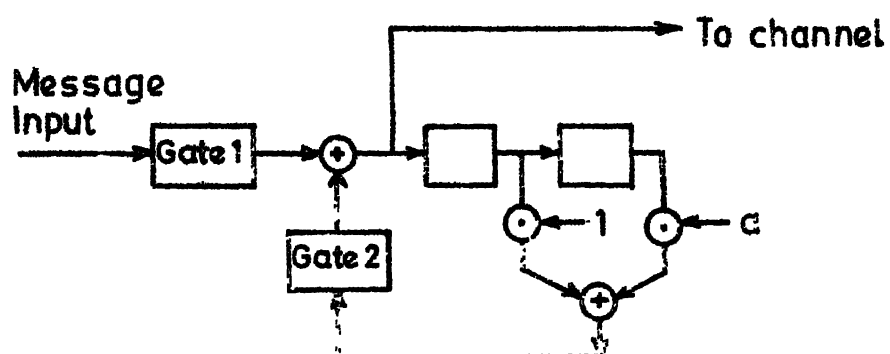


Fig 5.5.8a Encoder No.3 over $P_2^2[d^2+1]$ of Example 5.5.4

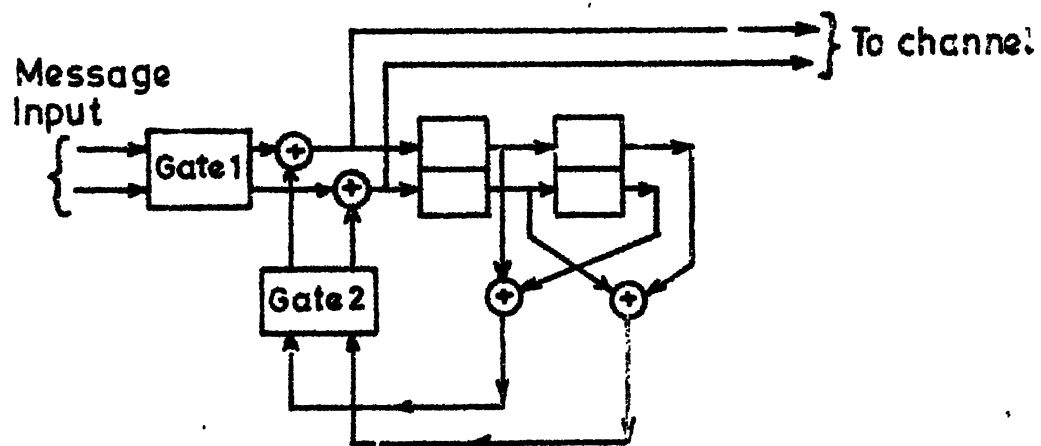


Fig 5.5.8b Encoder No.3 over $Z_2^2 \approx P_2^2[d^2+1]$ of Example 5.5.4

The minimum number of memory stages required for the generation of polynomial or cyclic codes over $P_p^n[W(a)]$ depends on the length of message words K and codewords N .

(i) In the case of Encoder No.1, $(N-K)$ memory stages are needed for implementing the encoder. Hence, this structure can be used for cases where $(N-K) < K$, to generate nonsystematic codes.

(ii) In the case of Encoder No.2, if the encoder is based on g_r^{-1} , $(N-K)$ memory stages are needed. If the encoder is based on g_o^{-1} , the number of memory stages needed are $(N-K)$ or K whichever is larger. Encoder No.2 based on g_r^{-1} can be used for cases where $(N-K) < K$, to generate systematic codes.

(iii) In the case of Encoder No.3 for generating systematic (N,K) cyclic codes, the number of memory stages needed are K . Hence, this encoder can be used when $(N-K) > K$.

5.5.2 Encoders for Interleaved Polynomial and Cyclic Codes

Interleaved codes [18-21, 53] are used to combat patterns of errors called burst errors, in which the error locations are

clustered together. We explain certain terms before taking up interleaved encoder structures corresponding to the basic encoders of previous subsection.

A burst of length b is a word where the only nonzero symbols are among b but not less than b successive symbols. An error word containing a burst of length b is called a burst error of length b .

Burst errors are common in channels which exhibit statistical dependence among successive transmitted symbols. They are called channels with memory. All practical channels except additive white Gaussian noise channels are of this type and degrade the performance of the codes designed to operate on memoryless channels. Even if the probability of single error is very low, the probability of another error immediately after any error occurs is large, which gives rise to burst error. As the effect of memory decreases with time separation, if all the symbols of a given codeword are transmitted at widely spaced intervals, the interleaving spaces being filled with similar symbols of other codewords, the effect of statistical dependence between the symbols of a codeword is eliminated and the burst error is randomised. Such codes are called interleaved

codes. The spacing interval in terms of symbols is called depth of interleaving.

In a linear code every burst error of length b or less may be detected iff no codeword is a burst of length b or less. Given an (N, K) linear code an interleaved $(\lambda N, \lambda K)$ code with depth of interleaving λ is constructed as follows. The λ codewords in the original code are arranged as λ rows of a rectangular arrays and then transmitted column by column as shown in Figure 5.5.9. A t error correcting code interleaved to a depth of λ can correct single bursts of length λt .

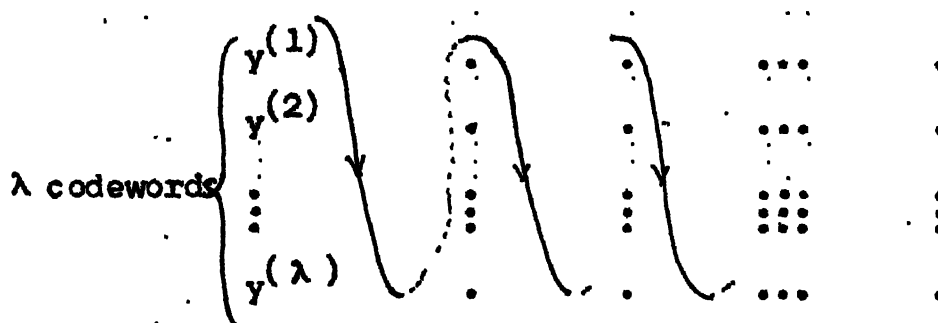


Figure 5.5.9 Transmission of Interleaved code

Thus one of the ways of implementing an interleaved code is to set up an arrays and operate on rows in encoding and decoding. In general this implementation may not be simple. If the generator polynomial of original code is $g(x)$ it can be shown that the generator polynomial of the interleaved code with interleaving depth λ , is $g(x^\lambda)$ [21]. Thus encoding of interleaved codes can be done using $P_p^n[W(a)]$ -LSS. The encoder

and decoder for the interleaved code can be derived from the encoder and decoder of the original code simply by replacing each register stage of the original encoder or decoder by stages with out changing other connections.

Interleaved Encoder No.1 : The encoder for generating interleaved nonsystematic polynomial or cyclic code is obtained by replacing each stage of the basic Encoder No.1 shown in Figure 5.5.1 by λ stages where λ is the depth of interleaving. The resulting scheme is shown in Figure 5.5.10 for the case (i) where the lowest degree symbol enters the encoder first. A similar structure can be worked out for case (ii) where the highest degree symbol enters the encoder first.

The characterising matrices of the LSS are

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}, \text{ a } \lambda(N-K) \times \lambda(N-K) \text{ matrix}$$

$$B = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ g_0 \end{bmatrix}, \text{ a } \lambda(N-K) \times 1 \text{ matrix}$$

$C = [g_r \ 0 \ \dots \ 0, g_{r-1} \ 0 \ \dots \ 0, g_1 \ 0 \ \dots \ 0]$, a $1 \times \lambda K$ matrix
and $D = [g_0 \ 0 \ \dots \ 0]$, a $1 \times \lambda$ matrix.

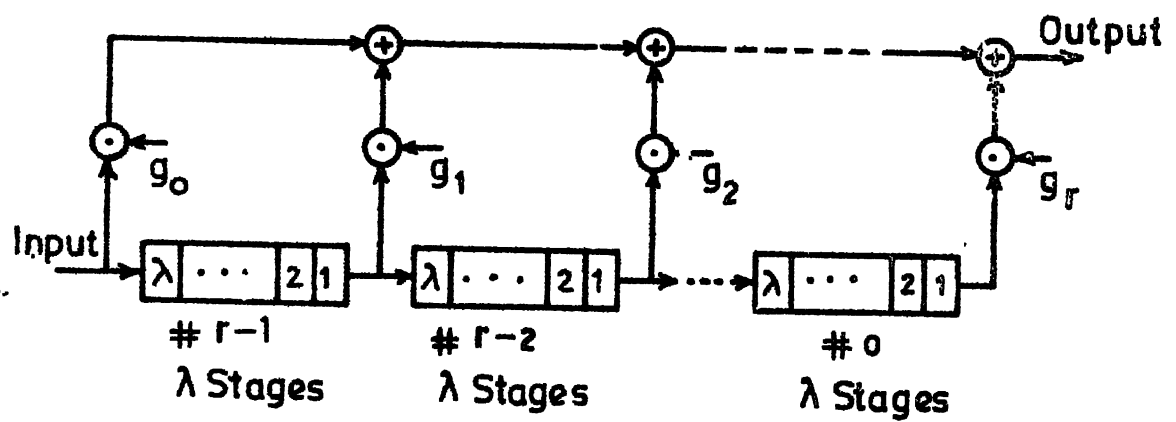


Fig.5.5.10 Interleaved Encoder No. 1

The operation is as follows :

Initially the contents of the memory devices are zeros. λK input symbols of the λ message words are given as input. At the same time the interleaved output symbols which are computed in the LSS are presented to the channel, whenever the message symbol from the i th message word is presented at the input, the output of the scalers correspond to the i th message word and hence the output symbol correspond to the i th codeword. $\lambda(N-K)$ zeros follow the λK message symbols at the input at the end of which the contents of the memory devices are cleared and next set of λK message symbols are given.

Example 5.5.5

Consider a $(3,1)$ polynomial code generated by $g(x) = a + (1+a)x + ax^2$ over $P_2[a^2+1]$. The interleaved Encoder No.1 with depth of interleaving 4 is given in Figure 5.5.11. The input is 4 message symbols followed by 8 zeros.

Let the message word be $u^{(1)} = (1+a)$, $u^{(2)} = a$, $u^{(3)} = 1$, $u^{(4)} = a$. The output is of length 12 and is

$$((1+a) \ 1 \ a \ 1 \ 0 \ (1+a) \ (1+a) \ (1+a) \ (1+a) \ 1 \ a \ 1)$$

The codeword if arranged columnwise as an array of 4-rows, each row is a codeword in the original $(3,1)$ code.

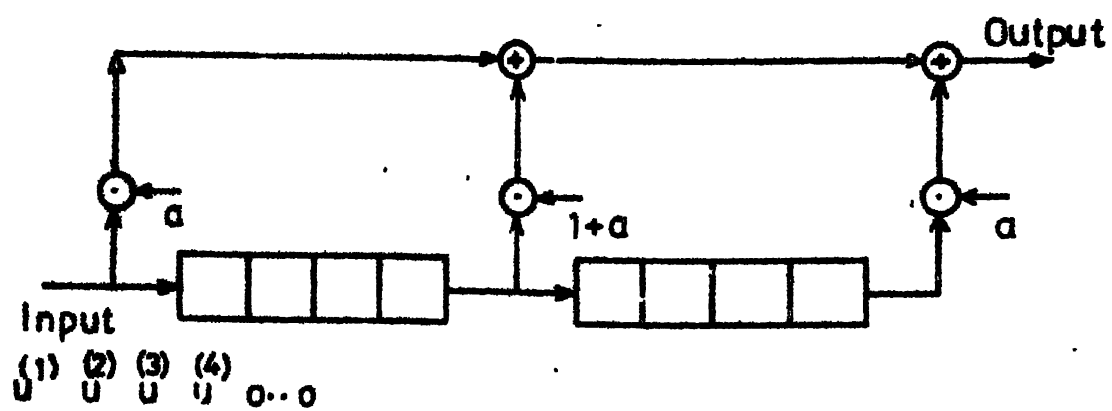


Fig.5.5.11 Interleaved Encoder No.1 of Example 5.5.5

$$\begin{array}{ccc}
 ((1+a) & 0 & (1+a)) \\
 (1 & (1+a) & 1) \\
 (a & (1+a) & a) \\
 (1 & (1+a) & 1)
 \end{array}$$

Interleaved Encoder No.2 : The encoder for generating interleaved systematic polynomial or cyclic codes is obtained by replacing each stage of the basic Encoder No.2 shown in Figure 5.5.3 or 5.5.4 by λ -stages where λ is the depth of interleaving. The resulting scheme is shown in Figure 5.5.12 for the case of Figure 5.5.3 based on g_r^{-1} . A similar structure based on g_o^{-1} can be worked out :

The operation is as follows :

With Gate 1 turned on and Gate 2 turned off the input of λK message symbols is given. Simultaneously, the message symbols are presented to the channel. During this interval the remainder of $x^{(N-K)} u^{(i)}(x)/g(x)$ corresponding to i th message word $u^{(i)}(x)$ is computed and the coefficients are stored at the i th location of each of the λ stage shift register; $i = 1, 2, \dots, \lambda$. The λK message symbols are followed by $\lambda(N-K)$ zeros. During this interval Gate 1 is turned off and Gate 2 is turned on and the interleaved parity check symbols are shifted to the channel.

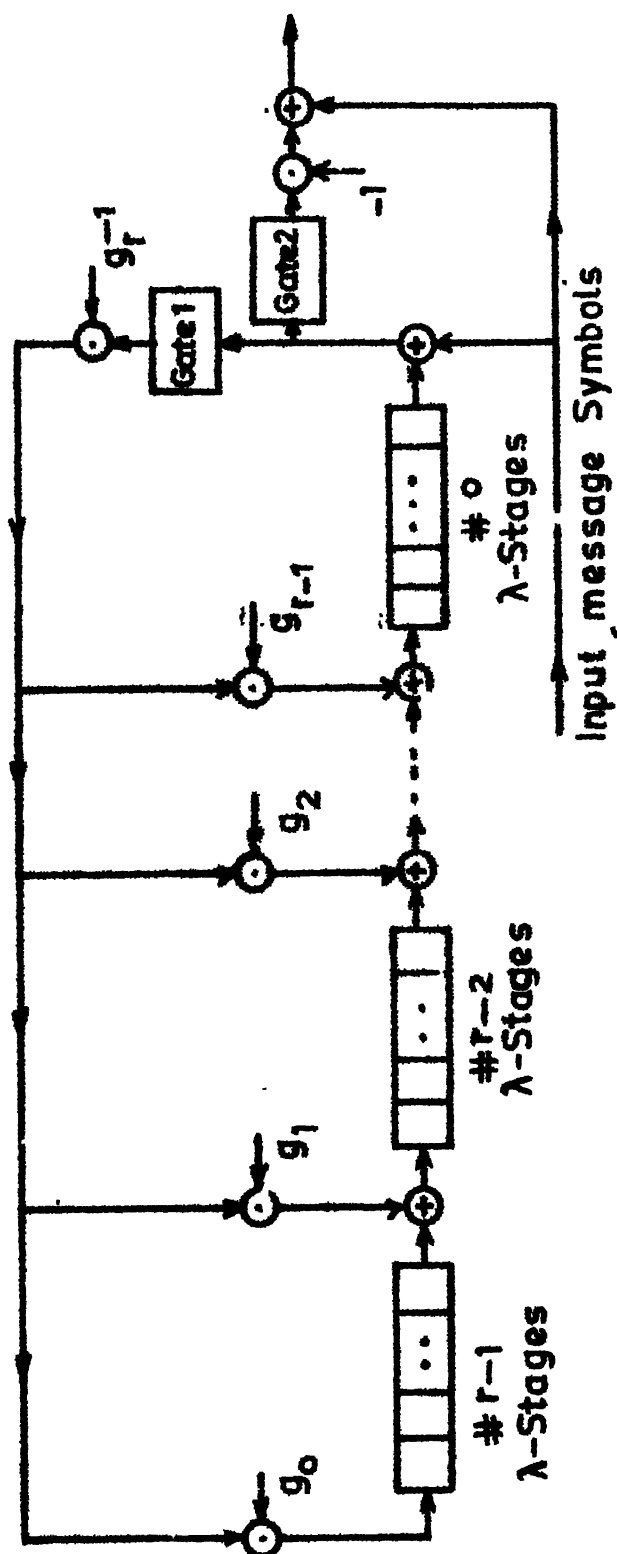


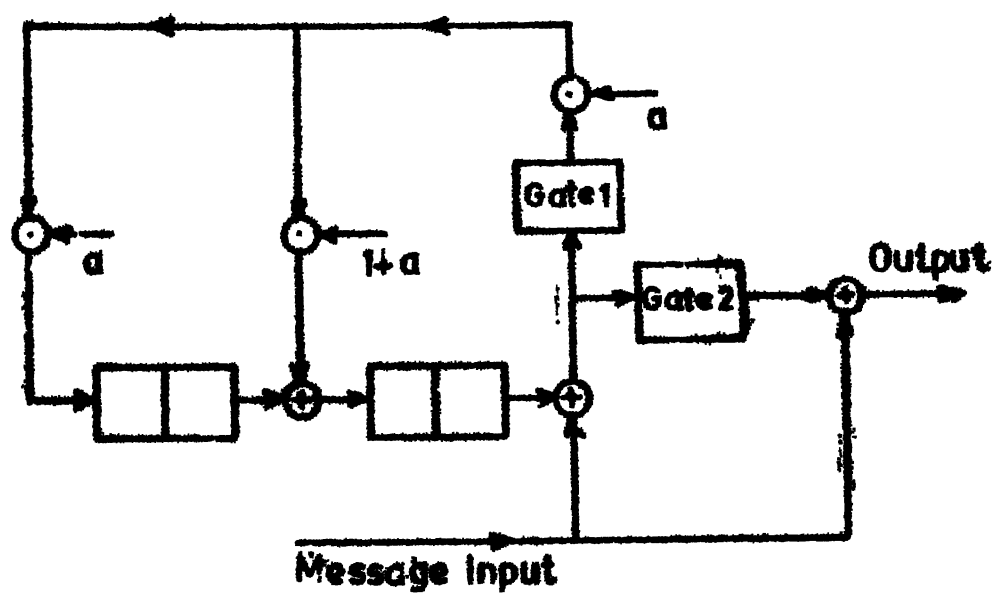
Fig-5.5.12 Interleaved Encoder No. 2

Example 5.5.6

Consider the systematic $(4,2)$ polynomial code over $P_2^2[a^2+1]$ of Example 5.5.2. The interleaved Encoder No.2 with depth of interleaving 2 is given in Figure 5.5.13. The input is 4 message symbols followed by 4 zeros. The implementation is based on g_r a unit.

Interleaved Encoder No.3

The encoder for generating interleaved systematic cyclic codes is obtained by replacing each stage of the basic Encoder No.3 shown in Figure 5.5.7 by λ -stages where λ is the depth of interleaving. The resulting scheme is given in Figure 5.5.14. The operation is as follows. Initially with Gate 1 turned on and Gate 2 turned off the λK message symbols are shifted into the encoder and the channel. The λK message symbols form the initial value of the LSS. The symbols corresponding to the i th message $u^{(i)}(x)$ are stored in the i th memory device in each of the λ -stage shift register. Then with the Gate 1 turned off and Gate 2 turned on the LSS is shifted $\lambda(N-K)$ times. During this interval the $\lambda(N-K)$ parity check symbols are generated and presented to the channel. At the end of this operation Gate 1 is turned on and Gate 2 is turned off, the next λK message symbols are shifted into the encoder and the operation is repeated.



**Fig. 5.5.13 Interleaved Encoder No. 2
Of Example 5.5.6**

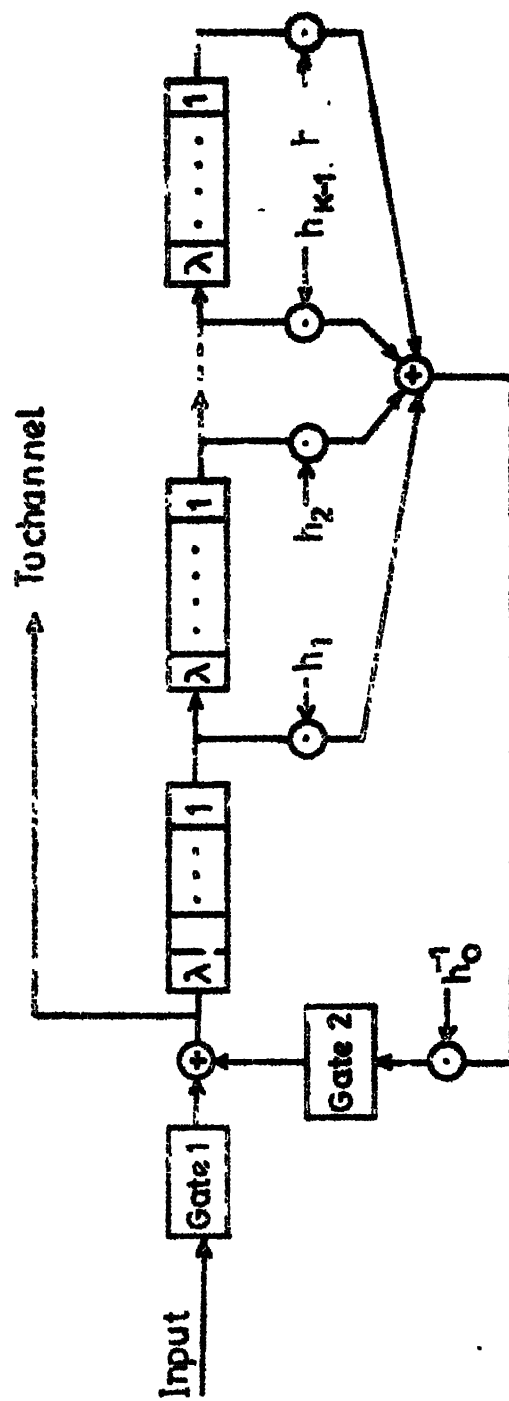


Fig. 5.5.14 Interleaved Encoder No.3

Example 5.5.7

Consider the $(6,2)$ cyclic code over $P_2^2[a^2+1]$ given in Example 5.5.1. For an interleaving depth equal to 2, interleaved Encoder No.3 is given in Figure 5.5.15a.

Let the message symbol input be $(u_0^{(1)} u_0^{(2)} u_1^{(1)} u_1^{(2)})$
 $= (1 \ a \ 0 \ a)$

followed by $\lambda(N-K) = 2(6-2) = 8$ zeros.

The interleaved codeword is

$(1 \ a \ 0 \ a \ a \ 1+a \ a \ a \ 1+a \ 1 \ a \ 0)$

which is the interleaved output of two codewords

$(1 \ 0 \ a \ a \ 1+a \ a)$ and $(a \ a \ 1+a \ a \ 1 \ 0)$.

The interleaved encoder over $Z_2^2 \cong P_2^2[a^2+1]$ is given in Figure 5.5.15b.

The corresponding message input over Z_2^2 is $(10 \ 01 \ 00 \ 01)$ followed by 16 zeros. The interleaved codeword is

$(10 \ 01 \ 00 \ 01 \ 01 \ 11 \ 01 \ 01 \ 11 \ 10 \ 01 \ 00)$ which is the interleaved output of two codewords.

$(10 \ 00 \ 01 \ 01 \ 11 \ 01)$ and $(01 \ 01 \ 11 \ 01 \ 10 \ 00)$.

The $(6,2)$ cyclic code over $P_2^2[a^2+1]$ has minimum weight 4.

Hence can correct single errors. Interleaved cyclic code with depth of interleaving 2, can hence correct a burst of length 2.

The corresponding cyclic code over Z_2^2 can correct all patterns of single errors and certain patterns of double errors. The

interleaved code can correct all patterns of bursts of length 2 and certain patterns of bursts of length 4.

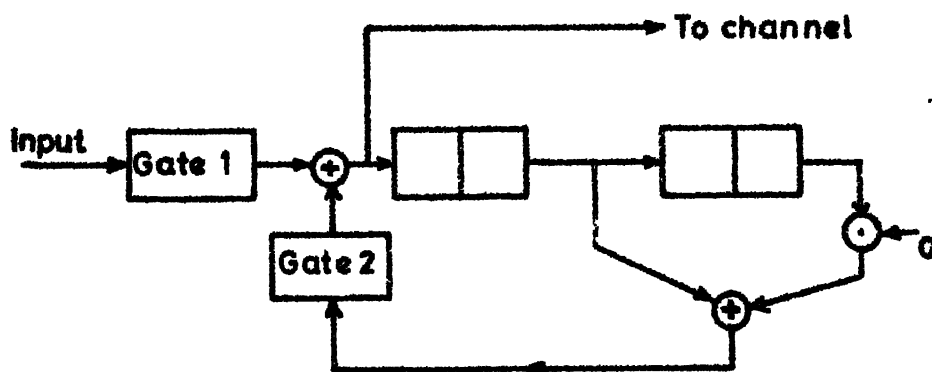


Fig.5.5.15a Interleaved Encoder No.3 over $P_2^2[a^2+1]$ of Example 5.5.4

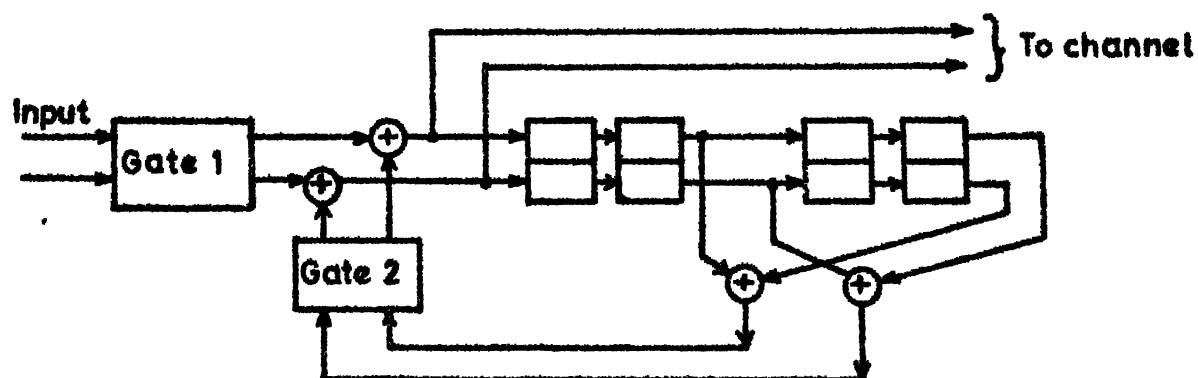


Fig 5.5.15b Interleaved Encoder No.3 over $Z_2^2 \times P_2^2[a^2+1]$ of Example 5.5.4

5.5.3 Serial Encoders for Polynomial and Cyclic Codes Over $P_p^n[a^n-1]$

We have considered basic and interleaved encoder structures for the generation of polynomial and cyclic codes over $P_p^n[W(a)]$. In all these implementations the ring operation is done in a parallel fashion. When the ring is $P_p^n[a^n-1]$ the properties of the ring can be made use of to give serial implementation of ring operations as discussed in Section 3.4. We have seen that $P_p^n[a^n-1]$ is isomorphic to the commutative ring of n -tuples Z_p^n in which the multiplication of two n -tuples corresponds to multiplication of an appropriate $n \times n$ cyclic matrix and an n -tuple. Thus if $g(x)$ and $u(x)$ are over $P_p^n[a^n-1]$ then the multiplication of the coefficients $g(x)$ and $u(x)$ can be regarded as multiplication of appropriate $n \times n$ cyclic matrices by n -tuples over $GF(p)$. This results in a simpler serial implementation compared to the parallel implementation. We call encoders with serial implementation of ring multiplication as serial encoders.

Serial implementation of multiplication of two elements from $P_2^n[a^n-1]$ requires only a cyclic shift register and one modulo 2 adder. This implementation is simpler compared to the serial multiplication of elements over $GF(2^n)$ proposed in [80] and used for encoding Reed-Solomon codes.

We consider serial Encoder Nos. 1 and 2, and 3 below.

Serial Encoder No. 1 : This encoder generates a nonsystematic polynomial or cyclic code over $Z_p^n[W] \simeq P_p^n[a^n-1]$. The message and codeword symbols are blocks of n -tuples over $GF(p)$. The generation of each component of n -tuple is serial. As in the case of basic Encoder No.1 two implementations are possible. Case i) where the feedforward coefficients are arranged as $(g_0 \ g_1 \ \dots \ g_r)$ and the n -tuple corresponding to lowest degree symbol of $u(x)$ enters the encoder first. In case (ii) the feedforward coefficients are arranged as $(g_r \ g_{r-1} \ \dots \ g_1 \ g_0)$ and the n -tuple corresponding to the highest degree symbol of $u(x)$ enters the encoder first. The scheme of case (i) is given in Figure 5.5.16.

The operation is as follows. Initially the contents of all the registers are zero. During the first n clock pulses the n components of the first message symbol u_0 is stored in the storage register. The output in the first interval of n clock pulses are n zeros. Before the $(n+1)$ th clock pulse the contents of storage register is transferred to register No. $(r-1)$ and contents of i th register is transferred to $(i-1)$ th register, $i = 1, 2, \dots, (r-1)$. During the next n clock pulses the second message symbol u_1 is stored in the storage register and contents of register No. 0 to $(r-1)$ are cyclic shifted. In the j th cyclic shift the j th digit of y_0 is computed. Thus there

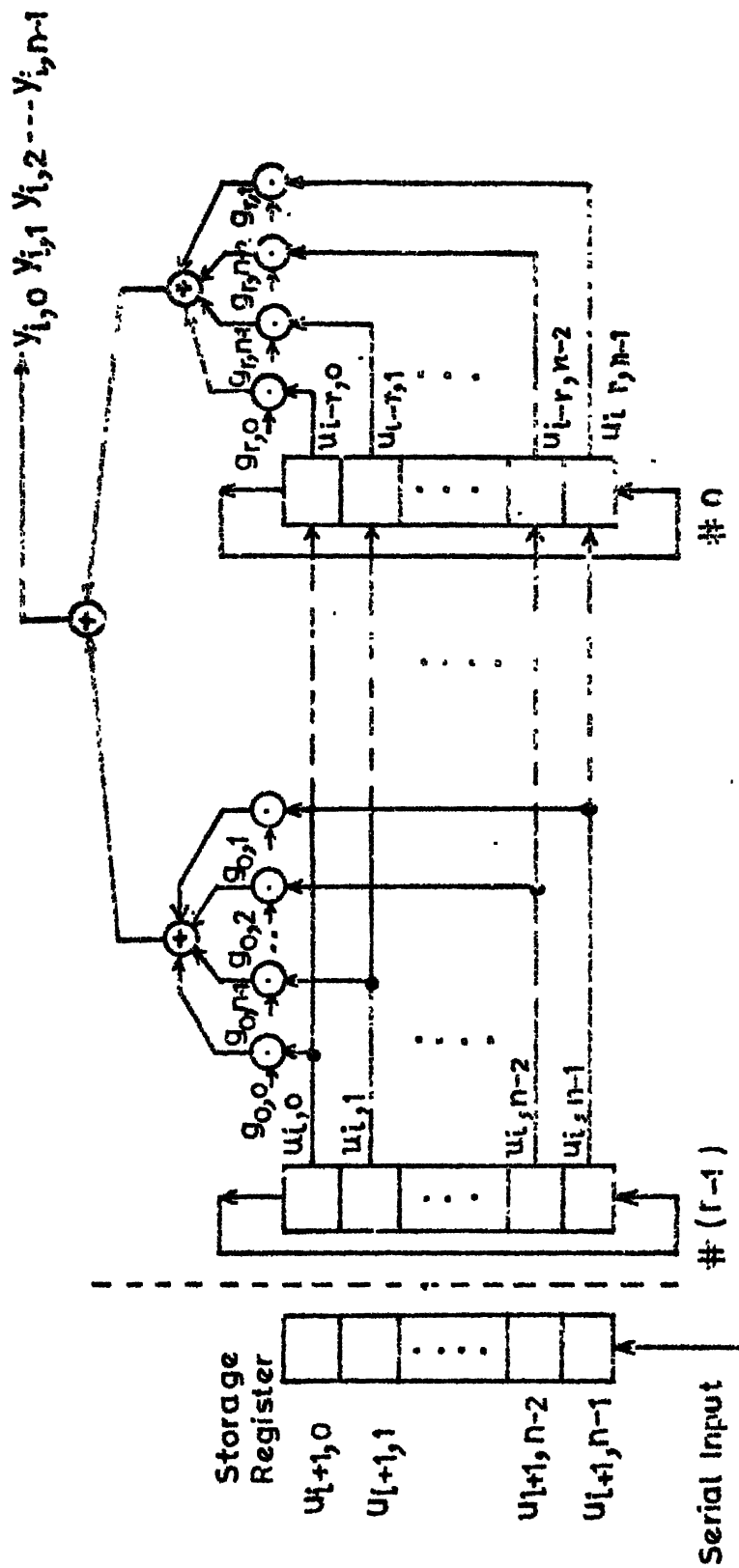


Fig. 5.5.16 Serial Encoder No.1

are two clocks; one to cyclic shift the contents of the cyclic shift registers and to compute the digits of the coefficients y_0, y_1, \dots , of $y(x)$, another clock to transfer the contents of the register. The rate of the transfer clock pulse is $1/n$ times the first one.

Serial Encoder No. 1 for case (ii) can be obtained in a similar fashion.

Serial Encoder No.2 : This encoder generates systematic polynomial or cyclic code over $Z_p^n[W] \cong P_p^n[a^n-1]$. The message and codeword symbols are blocks of n -tuples over $GF(p)$. The encoding operation is serial. As in the case of basic Encoder No.2 two implementations are possible, case (i) is based on g_r a unit in $P_p^n[a^n-1]$ and case (ii) g_o a unit in $P_p^n[a^n-1]$. In the first case n tuple corresponding to the highest degree symbol, u_{K-1} of the message enter the encoder first. This case is discussed below and the scheme is given in Figure 5.5.17. A similar structure of Encoder No.2 based on g_o a unit in $P_p^n[a^n-1]$ can be obtained on the same lines.

Each memory device of Encoder No.2 given in Figure 5.5.3 is replaced by a bank of n memory devices over $GF(p)$ the scalars are appropriately chosen from $GF(p)$. The operation is as follows. With Gate 1 turned on and Gate 2 turned off input of nK message digits are given in blocks of n digits over $GF(p)$. When a block of n -tuple is shifted into the encoder, it is

stored in storage shift register u and simultaneously presented to the channel. Before the next clock pulse, contents of storage register u is transferred to the cyclic shift register. Multiplication by coefficients is effectively modulo p addition of scaled digits of appropriate locations in the cyclic shift register. This is shown schematically in the Figure 5.5.17. The set of scalars $(g_{i,0}^1, g_{i,1}^1, \dots, g_{i,n-1}^1)$ over $GF(p)$ corresponds to the scalar $g_i^1 = -g_i g_r^{-1}$; $i = 0, 1, 2, \dots, r-1$, over $P_p^n[W(a)]$. The successive components of the product are generated when the contents of cyclic shift registers are shifted. These components are shifted into appropriate locations in the n stage shift registers of the $r = (N-K)$ stages. During the interval when n digits of the product are computed and feedback, second block of n digits would have been stored in the storage register and simultaneously presented to the channel. The contents of the storage register is then transferred to the cyclic shift register and the process continues.

At the end of nK clock pulses the r, n -stage shift registers contain the remainder of the division in serial form. For the remaining period of $n(N-K)$ clock pulses, the input is a sequence of $n(N-K)$ zeros. The contents of the LSS is then shifted to the channel with Gate 1 turned off and Gate 2 turned on.

Serial Encoder No.3 : This encoder generates systematic cyclic codes over $Z_p^n[W] \simeq P_p^n[a^n-1]$. The message and codeword symbols

are blocks of n -tuples over $GF(p)$. The encoding operation is serial. Serial Encoder No.3 can be obtained from basic Encoder No.3 given in Figure 5.5.7, by replacing each memory device by n -stage shift registers over $GF(p)$. The scalars are appropriately chosen from $GF(p)$. The implementation of the encoder is given in Figure 5.5.18. Here h_0 is assumed to be 1.

The nK message symbols are loaded into the encoder as follows. With Gate 1 turned on and Gate 2 turned off the nK digits of the K message symbols are shifted into the encoder and the channel simultaneously. In each block of n -clock pulses the input n digits are stored in the storage register serially and then transferred to the shift register No. $(K-1)$, in parallel. At the same time the contents of register No. i is transferred to No. $(i-1)$, $i = 1, 2, \dots, (K-1)$. During each n clock intervals the cyclic shift register contents are cyclically shifted and at each shift the corresponding feedback digit is computed. However, when the message digits are being shifted at the input, since Gate 2 is turned off the feedback digits will not appear at the input of n -stage storage register. When all the nK message symbols are loaded into the encoder Gate 1 is turned off and Gate 2 is turned on. Now the contents of the LSS are the message symbols which are the initial values. During the remaining $n(N-K)$ clock pulses the $n(N-K)$ parity check digits are formed and presented to the channel. Then Gate 1 is turned on and Gate 2 is turned off and next set of nK message digits are shifted into the encoder.

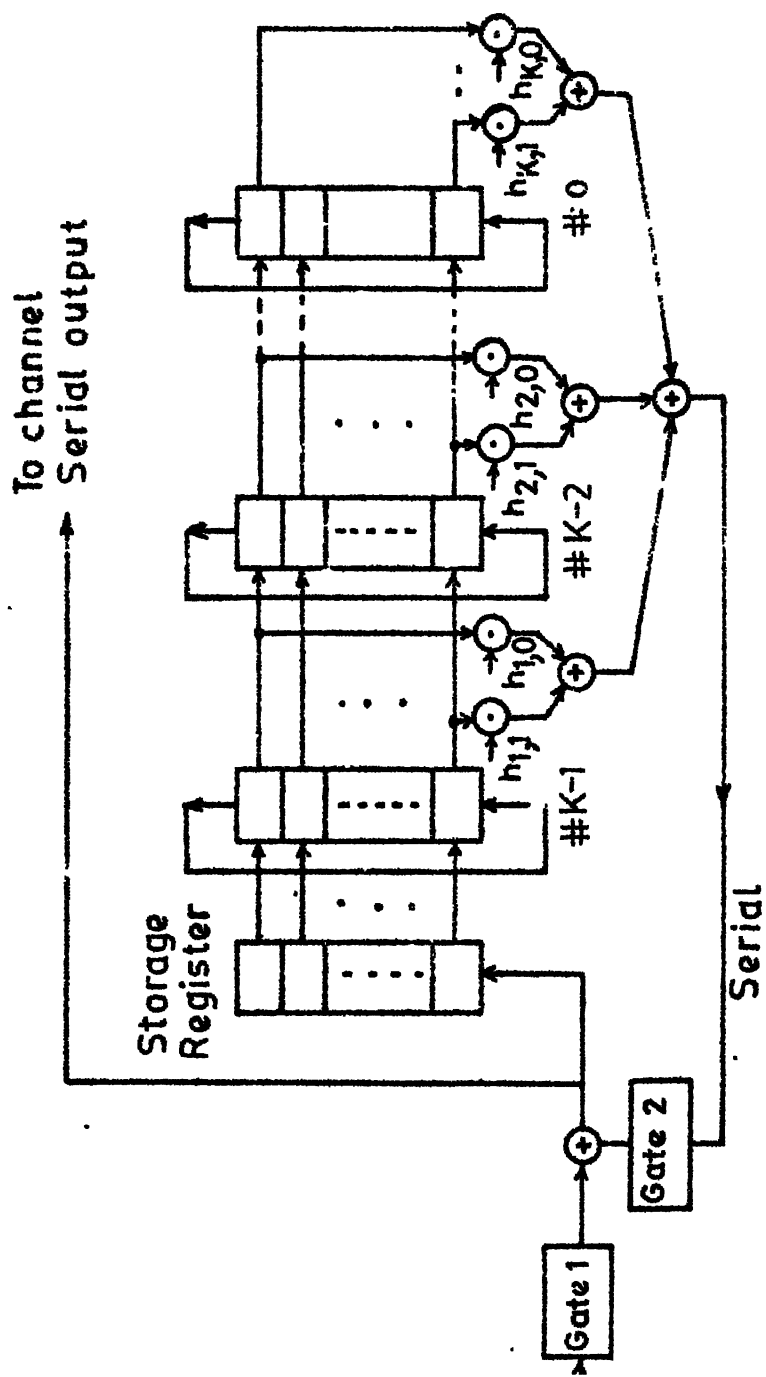


Fig. 5.5.18 Serial Encoder No. 3

5.5.4 Serial Interleaved Encoders

In this section we give three serial interleaved encoders corresponding to the three serial encoders of previous subsection.

Serial Interleaved Encoder No. 1 : This encoder generates an interleaved nonsystematic polynomial or cyclic code over $\mathbb{Z}_p^n[W] \cong \mathbb{P}_p^n[a^n-1]$ and is obtained by replacing each stage of the serial Encoder No.1 shown in Figure 5.5.16 by λ stages. The resulting scheme is shown in Figure 5.5.19 for the case where the lowest degree symbol of input enter the encoder first. A similar structure can be worked out for the other case. Each block in the Figure 5.5.19 represents an n -stage shift register. The input is a serial input of λnK digits followed by $\lambda n(N-K)$ zeros over $\text{GF}(p)$. Every λ th n -tuple corresponds to the same message word. The operation is as follows. Initially the contents of the memory devices are zeros. When the first n -tuple is presented at the input the output is a sequence of n zeros. At the end of input of a block of n -tuple of first message, the contents of the first shift register in each stage is transferred to the n stage cyclic shift register. During the time, next block of n -tuple corresponding to the second message arrives at the input, the contents of n stage shift registers in each stage are shifted to the next one and the digits of the product of n -tuples

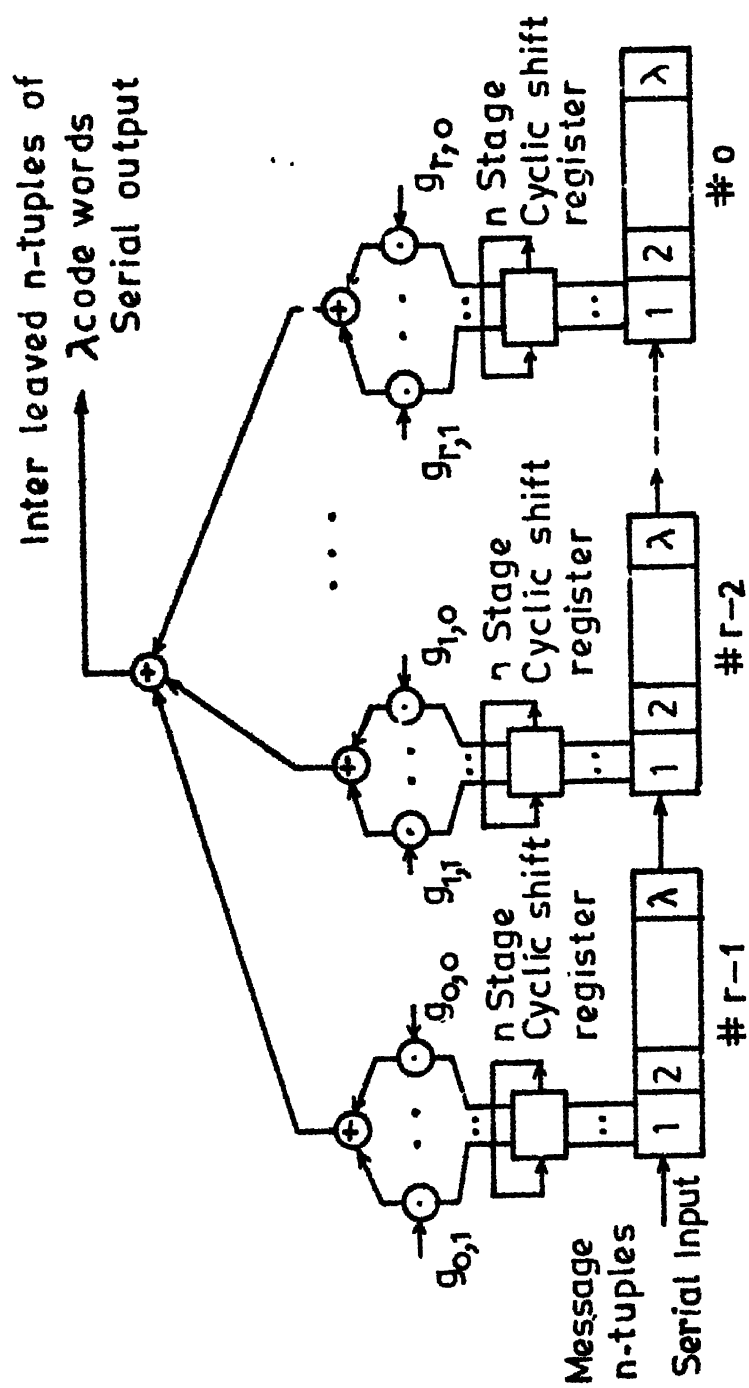


Fig. 5.5.19 Serial Interleaved Encoder No.1

corresponding to g_1 and the n -tuple corresponding to the message symbol are computed by cyclic shifting the contents of cyclic shift register and adding the appropriate scaled digits. The digits corresponding to the product appears at the output.

Serial Interleaved Encoder No.2 : This encoder generates an interleaved systematic polynomial or cyclic codes over $Z_p^n[W] \cong P_p^n[a^n-1]$. As in the case of basic Encoder No.2 two structures are possible based on g_r a unit or g_o a unit. The serial interleaved Encoder No.2 is obtained by replacing each stage of the serial Encoder No.2 shown in Figure 5.5.17 by λ stages. The resulting scheme is shown in Figure 5.5.20 for the case g_r a unit. A similar structure can be worked out for the case g_o a unit.

Each block in the Figure 5.5.20 represents an n -stage shift register. As in the case of Serial Interleaved Encoder No. 1 the input is a serial input of λnK digits followed by λnK zeros over $GF(p)$. Every λ th n -tuple corresponds to the same message word. The operation is as follows. Initially with Gate 1 turned on and Gate 2 turned off. λnK message digits go to the channel and the encoder simultaneously. These digits correspond to the K message symbols of λ messages. After all the λnK message digits are shifted, Gate 1 is turned off and Gate 2 is turned on. During the remaining period of $\lambda n(N-K)$ clock cycles the input is $\lambda n(N-K)$ zeros. Now the

n digit cyclic shift register
n digit Storage register

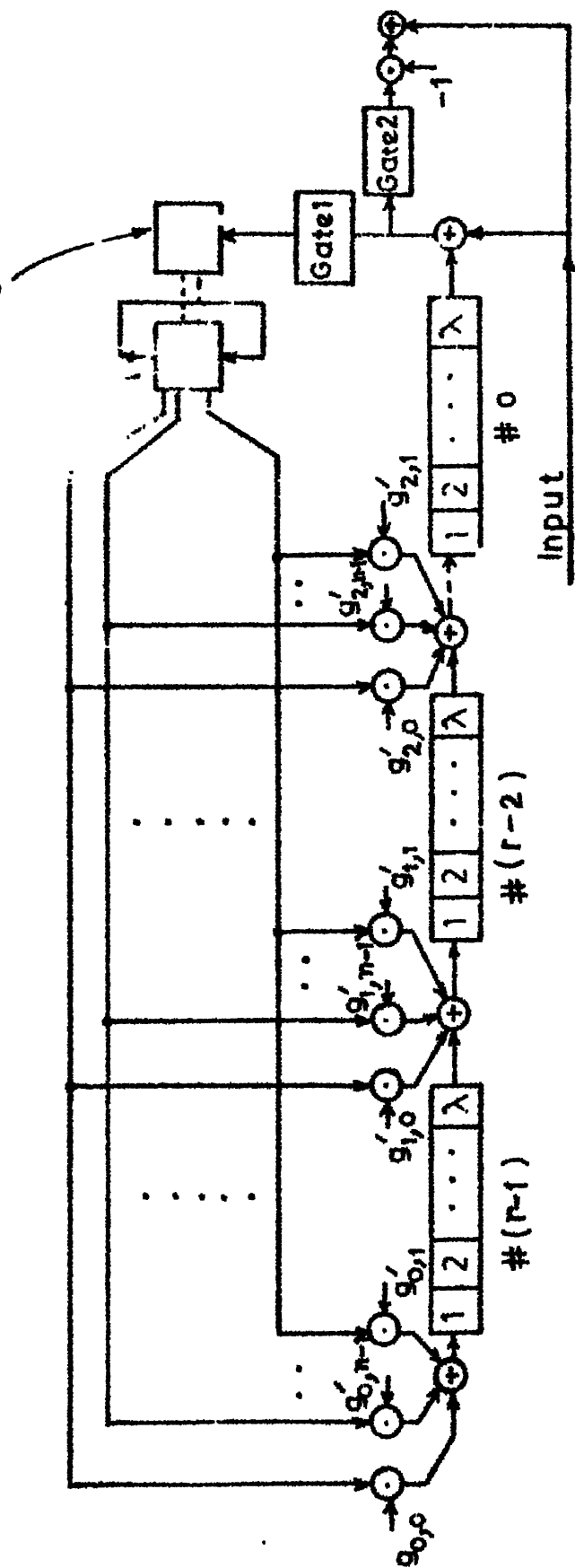


Fig. 5.5.20 Serial Interleaved Encoder No.2

remainder digits which have been computed and are available in the memory devices are presented to the channel. Every λ th n -bit block correspond to the same codeword.

The multiplication by scalars in the feedback is facilitated by the n -digit cyclic shift register and appropriate modulo p scalars and adders. For example the set of scalars $(g'_{0,0}, g'_{0,1}, \dots, g'_{0,n-1})$ over $GF(p)$, associated with the modulo p adder at the input of $(r-1)$ th stage corresponds to the scalar $g_0^{-1} = -g_0 g_r^{-1}$.

Serial Interleaved Encoder No.3 : This encoder generates interleaved systematic cyclic codes over $Z_p^n[W] \cong P_p^n[a^n-1]$ and is obtained by modification of the serial Encoder No.3 shown in Figure 5.5.18. Each first n stage register in the λ stages is associated with an n -stage cyclic shift register. The multiplication by coefficients h_i is implemented serially by adding the scaled contents at the appropriate locations of the n -stage cyclic shift register. The resulting scheme is shown in Figure 5.5.21. Each block in the figure represents an n -stage shift register over $GF(p)$. The input is a serial input of $\lambda n K$ digits of λ messages. Every λ th n -tuple correspond to the same message. The operation is as follows :

With Gate 1 turned on and Gate 2 turned off input sequence of λK blocks of n digits corresponding to λ interleaved message symbols is given simultaneously to the channel and the encoder.

When the n -digit shift register No. 1 is stored with an n -tuple, it is loaded into the cyclic shift register also. The feedback digits are computed by cyclically shifting the contents of the cyclic shift register and adding modulo p , of appropriate scaled digits. After shifting the λnK message digits Gate 1 is turned off and Gate 2 is turned on. During the remaining $\lambda n(N-K)$ clock interval the $\lambda n(N-K)$ check digits are computed and presented to the channel.

Example 5.5.8

Consider the encoding of a $(15,2)$ systematic linear cyclic code over $P_2^3[a^3-1]$ using Encoder No.3. A nonsingular, autonomous, single output canonical $P_2^3[a^3-1]$ -LSS with feedback polynomial $h(x) = 1+x+ax^2$ generates the code and scheme is given in Figure 5.5.22a. As seen in Example 4.4.13 the period of the autonomous response is a divisor of 15 and the minimum weight is 10. Hence the code can correct all patterns of 4 symbols over $P_2^3[a^3-1]$.

Serial Implementation : The serial implementation of the above encoder is given in Figure 5.5.22b. $(15,2)$ linear cyclic code over $Z_2^3 \cong P_2^3[a^3-1]$ is a $(45,6)$ code over $GF(2)$. The code has the following error correcting capabilities :

- i) All patterns of burst errors of length $(4-1) \times 3 = 9$ bits
- ii) All patterns of single errors of length 4 bits.

Serial Interleaved Implementation :

The scheme is given in Figure 5.5.22c. Depth of interleaving is 2. The code is a $(80,12)$ over $Z_2^3 \cong P_2^3[a^3-1]$ and has the following error correcting capability :

- (1) all patterns of burst errors of length 18 bits and
- (2) all patterns of single errors of length 8 bits.

5.6 DECODERS FOR POLYNOMIAL AND CYCLIC CODES OVER $P_p^n[W(a)]$

In this section we consider decoder structures for polynomial and cyclic codes. Three decoders are given. The first one incorporates the syndrome decoding. It is basically a LSS which performs polynomial division to compute syndrome and makes use of decoding table for decoding the received word. This decoder is suitable for both polynomial and cyclic codes. The other two decoders viz. permutation decoder and Hamming cross correlation decoder whose principles are given in Section 5.4 can be employed to decode cyclic codes over $P_p^n[W(a)]$. Hamming cross correlation decoder can be used for any cyclic code while permutation decoder can be used only for systematic cyclic codes.

5.6.1 Decoders based on Polynomial Division

An (N,K) polynomial or cyclic code C is such that every codeword is a multiple of a generating polynomial $g(x)$ of degree $r = (N-K)$. At the receiver the received word $y'(x)$ is divided by $g(x)$. A nonzero remainder indicates an error. There is a

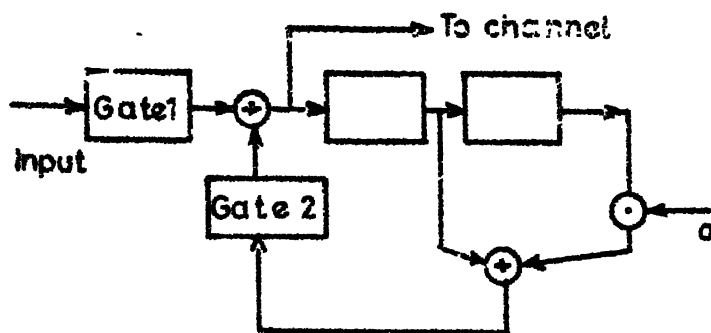


Fig.5.5.22 a Encoder No.3 of Example 5.5.7

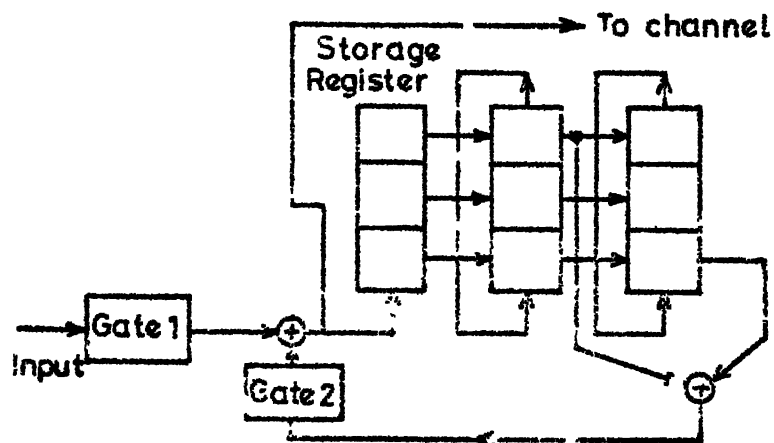
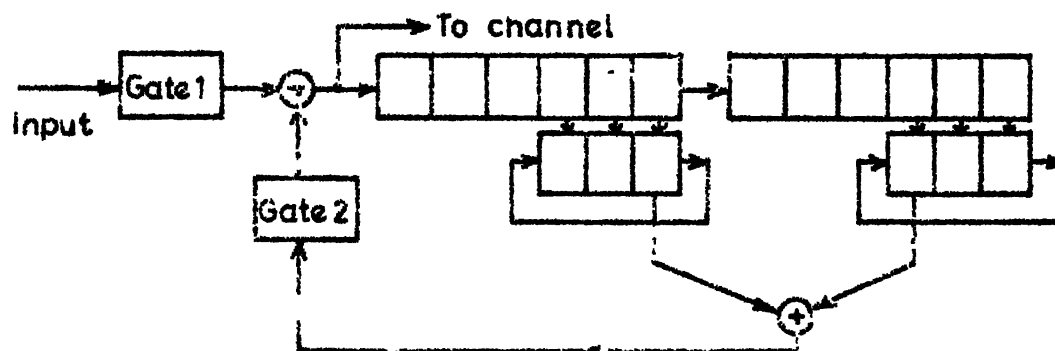


Fig.5.5.22 b Serial Encoder No.3 of Example 5.5.7

Fig.5.5.22 c Serial Interleaved Encoder No.3
of Example 5.5.7

one-to-one correspondence between the remainder and the coset leader, in the cosets of C in the group of all polynomials of degree $(N-1)$ or less. The coset leader corresponding to the remainder is found and subtracted from $y'(x)$ to get the transmitted word. Two polynomial division circuits incorporating g_0^{-1} or g_r^{-1} with proper sequence of input codeword symbols are possible. First we consider the division circuit based on the premise that g_0 a unit. As we have seen earlier in Section 5.3 the lowest degree term first enters the decoder.

Polynomial division by $g(x)$ of degree r is implemented by an r th order feedback LSS whose feedback coefficients depend on the coefficients of $g(x)$. The LSS is given in Figure 5.6.1. The LSS for division of polynomials over finite field is given in [12].

The initial content of the shift registers is zero. At the end of $N-1$ shifts the contents of the register is the remainder.

As we are interested only in the remainder, the LSS can be modified as in Figure 5.6.2.

The characterising matrices of the LSS given in Figure 5.6.2 are

$$A = \begin{bmatrix} -g_1 g_0^{-1} & 1 & 0 & 0 & \dots & 0 \\ -g_2 g_0^{-1} & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & & \vdots \\ -g_{r-1} g_0^{-1} & 0 & 0 & 0 & \dots & 1 \\ -g_r g_0^{-1} & & 0 & 0 & \dots & 0 \end{bmatrix}$$

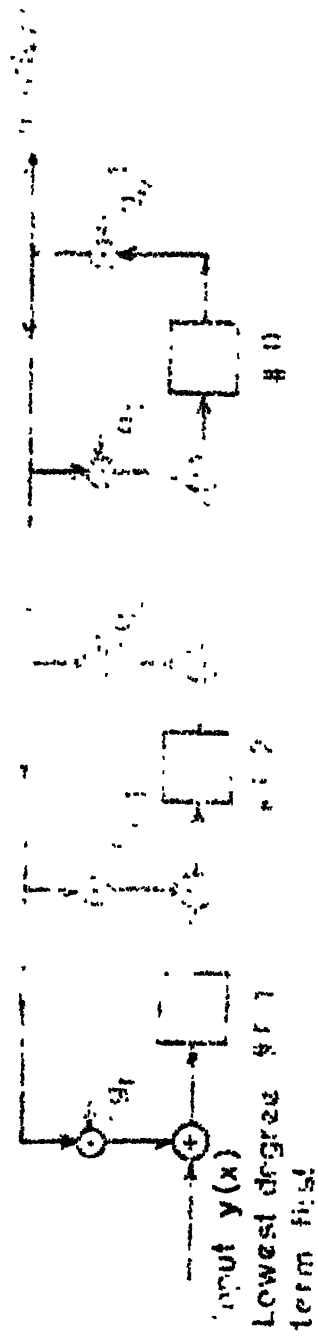


Fig. 5.6.1 LSS for Polynomial Division based on g_0 a unit

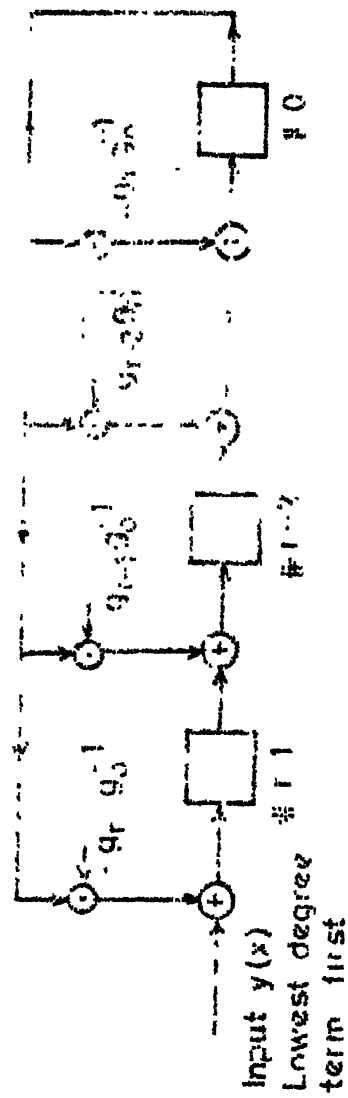


Fig. 5.6.2 Modified LSS for Polynomial Division

$$B = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

Implementation over $Z_p^n[W]$ can be obtained, using the isomorphism between $P_p^n[W(a)]$ and $Z_p^n[W]$ given in Section 2.3 when the coefficients g_i and y_i are from $P_p^n[a^n-1]$ serial implementation of the division circuit given in Figure 5.6.3 is possible. The input to the i th exclusive-OR gate are appropriate scaled components from the cyclic shift register, which are determined from the coefficients of the scaler

$$g_i^1 = -g_{i+1}g_0^{-1} = (g_{i,0}^1, g_{i,1}^1, \dots, g_{i,n-1}^1) ; i = 1, 2, \dots, r.$$

At the end of $n.(N-1)$ shift pulses if the contents of all the shift registers are zero, there is no error in the received polynomial. A nonzero remainder indicates an error and correction is done by subtracting the coset leader corresponding to the remainder polynomial, from the received polynomial. The decoder based on g_r a unit in $P_p^n[W(a)]$ is given below which is a $P_p^n[W(a)]$ -LSS, and perform division by $g(x)$ as in the earlier case. The scheme is given in Figure 5.6.4. The operation is identical to the division circuit considered earlier. However in this case the highest degree symbol of the received word polynomial enters the decoder first.

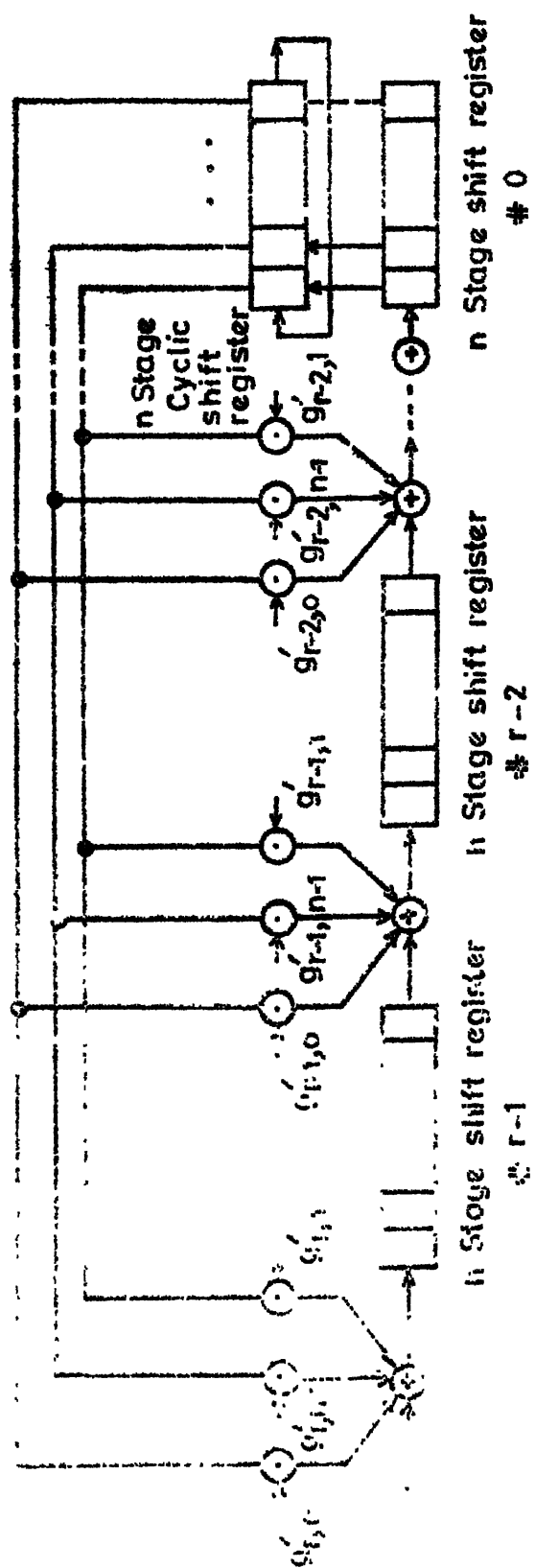


Fig 1.6.3 Serial Implementation of Polynomial division .

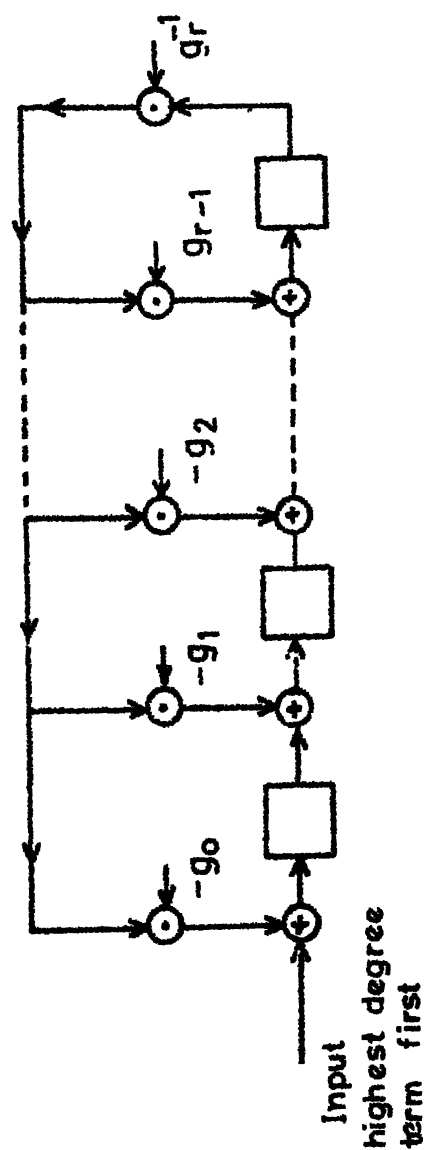


Fig. 5.6.4 LSS for Polynomial division based on g_r a unit.

5.6.2 Permutation Decoder for Systematic Cyclic Codes

As seen in Subsection 5.4.3 the principle of permutation decoder is that the Hamming distance between the two codewords y and z is unaltered with cyclic shifts by the same amount.

For decoding (N,K) systematic cyclic codes we make use of N LSS which are all identical to the encoder at the transmitter. The scheme is given in Figure 5.6.5. The received word is stored in an input buffer. Each successive K symbols \bar{y}' , $\overline{\sigma y'}$, ..., $\overline{\sigma^{N-1} y'}$ of the received word as input to the N encoders, the corresponding codewords of length N , $\overline{E(y)}$, $\overline{E(\sigma y')}$, ..., $\overline{E(\sigma^{N-1} y')}$ are generated. Each sequence is compared with the appropriate shifted version of the received sequence and the distances are computed. The sequence which is nearest to the appropriate shifted version of the received word is the shifted version of correct sequence. An equal amount of inverse cyclic shift of the locally generated codeword is the most likely transmitted codeword.

5.6.3 Decoder Based on Hamming Cross Correlation Properties of Cyclic Codes

The principle of this decoder is given in Subsection 5.4.3. Here we give the schematic arrangement illustrated in Figures 5.6.6a and 5.6.6b.

Let the cyclic code C have μ distinct codewords which are obtained from the cycle length decomposition of the states of

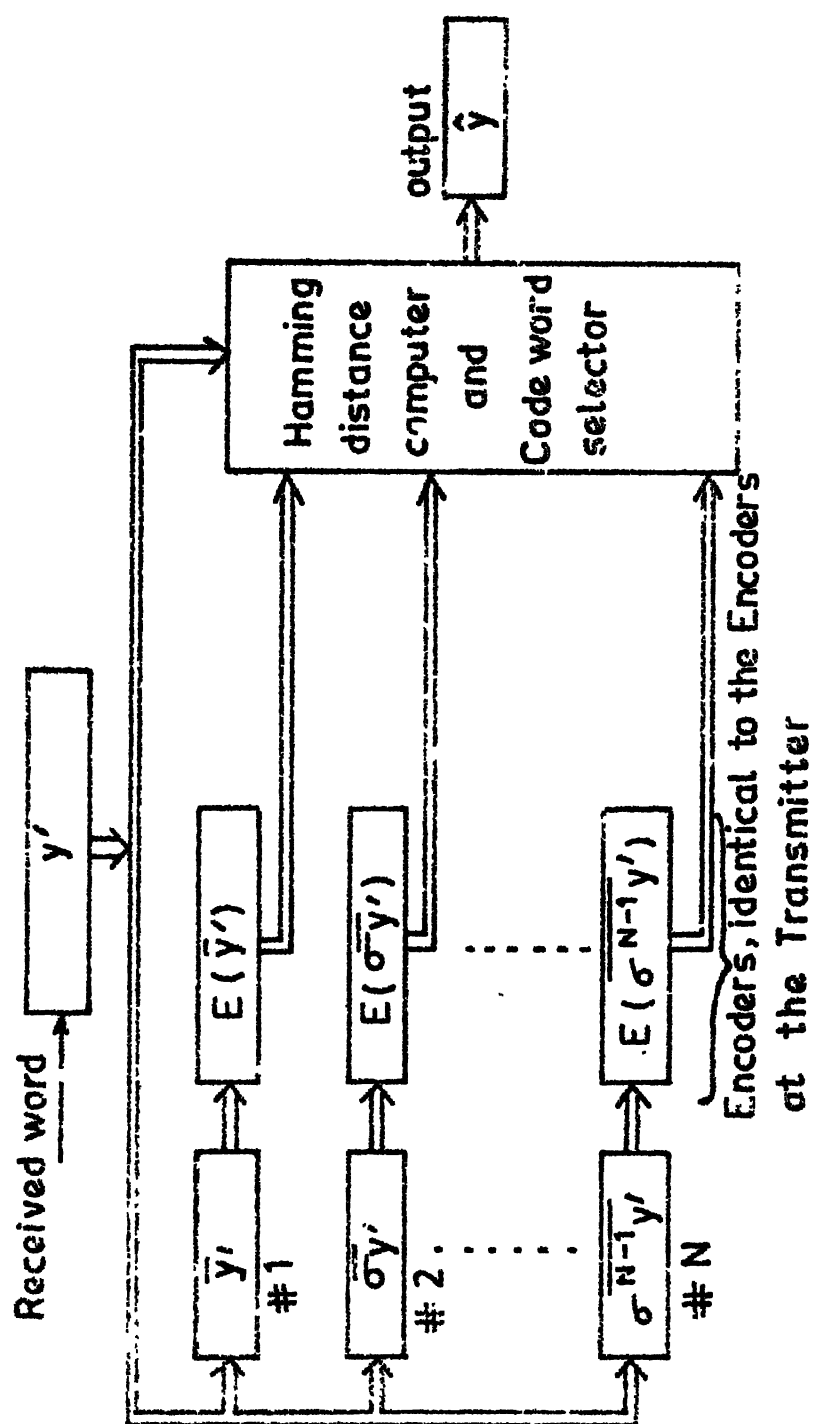


Fig. 5.6.5 Schematic Diagram of Permutation Decoder.

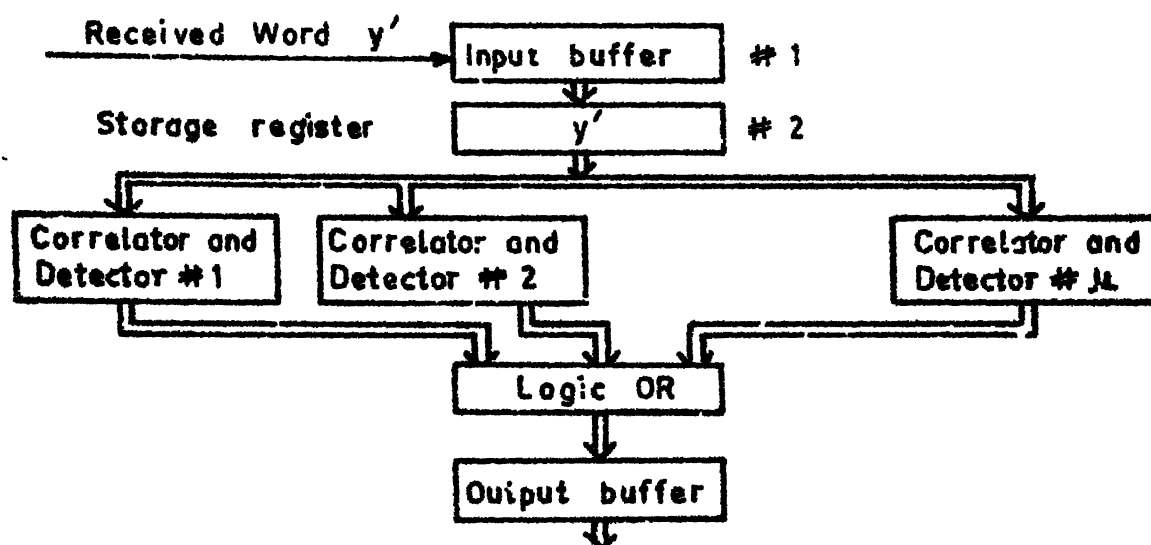


Fig. 5.6.6a Hamming Cross-correlation Decoder.

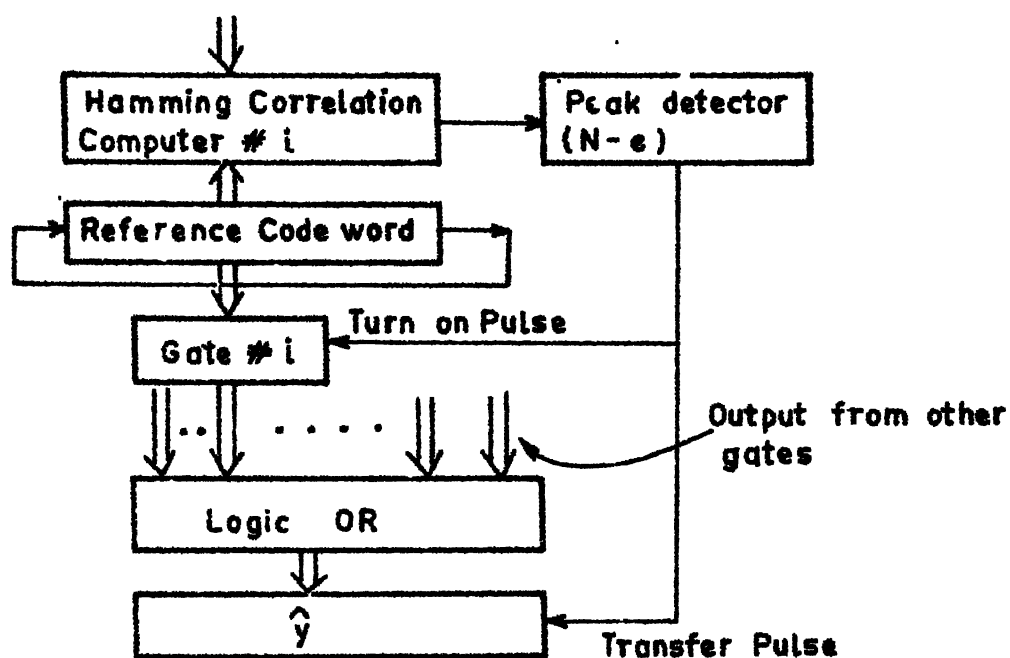


Fig. 5.6.6b Correlator and Detector of Hamming Cross-correlation Decoder

associated LSS. The received word which is stored in input buffer is transferred to the register 2, at the commencement of decoding of word y' . During the decoding of the word y' , the input buffer will be storing the next codeword. The Hamming distance between the received word and each shifted version of reference word is computed in the μ correlators for shifts, $\tau = 0, 1, \dots, N-1$. The peak detector associated with each correlator monitors the peak value of the Hamming cross correlation (HCCR) function between the received word y' and the shifted version of reference word. When the HCCR function value exceeds $(N-e)$, where e is the error correcting capability of the code, the gate associated with that reference codeword is enabled and the contents which is the decoded word is transferred to output buffer, before the next clock pulse. Decoding time is atmost N clock pulses. The details of a correlator and detector are given in Figure 5.6.6b.

At the end of N clock pulses after the commencement of decoding of a received word, the decoded word is available at the output buffer. Meanwhile second codeword would have been stored in the output buffer which is transferred to register 2 and decoding of this word commences and the process repeats. We note here that the decoding delay is one codeword.

The decoders given in the foregoing sections can also be used for decoding interleaved codes by first separating the λ

codewords where λ is the depth of interleaving and then independently decoding them. Alternatively a decoder for decoding interleaved codes directly can also be obtained by replacing each stage of the decoder by λ stages.

CHAPTER 6

CONCLUSION

In this thesis we have presented the theory and applications of a generalised version of linear sequential systems (LSS). These are LSS over rings of residue class polynomials over $GF(p)$, modulo a polynomial $W(a)$ of degree n . Such rings, denoted by $P_p^n[W(a)]$, are commutative rings of order p^n with identity. LSS over $P_p^n[W(a)]$ are denoted by $P_p^n[W(a)]$ -LSS. LSS over finite fields are a specific case of $P_p^n[W(a)]$ -LSS; when $W(a)$ is irreducible over $GF(p)$, $P_p^n[W(a)]$ becomes $GF(p^n)$ and we get $GF(p^n)$ -LSS. The results given in this thesis can, therefore, be regarded as a generalisation of the results on $GF(p^n)$ -LSS. The implementation aspects and analysis of $P_p^n[W(a)]$ -LSS have been studied and the applications of $P_p^n[W(a)]$ -LSS for generation of sequences over $P_p^n[W(a)]$, modulation and multiplexing of digital data and encoding and decoding circuits for error control coding are given.

$P_p^n[W(a)]$ -LSS, like $GF(p^n)$ -LSS, are described in terms of state and output equations. In the case of an m -input, j -output, K th order $P_p^n[W(a)]$ -LSS, the set of input m -tuples, the set of output j -tuples and the set of state K -tuples constitute $P_p^n[W(a)]$ -modules of rank m, j and K respectively. Although the basic description and consequently the analysis

procedures of $P_p^n[W(a)]$ -LSS are identical to that of $GF(p^n)$ -LSS, the properties of the former differ significantly because of differences in structural properties of $P_p^n[W(a)]$ and $GF(p^n)$. First of all it is noted that in a finite ring, unlike a finite field, the notion of multiplicative inverse does not exist for elements which are zero divisors. Secondly, it is noted that, in contrast to finite fields, all the commutative rings of the same order are not isomorphic to each other; even residue class polynomial rings of the same order are not isomorphic to each other. The set of all isomorphic residue class polynomial rings of any given order constitutes an equivalence class and each equivalence class of residue class polynomial rings gives rise to a distinct class of LSS. $GF(p^n)$ -LSS belong to one such class. Key results obtained in the thesis are summarised below.

6.1 SUMMARY OF RESULTS

$P_p^n[W(a)]$ have been classified into finite fields local rings semisimple rings or semilocal rings depending on the prime factorisation of the modulus polynomial $W(a)$. Decompositions of $P_p^n[W(a)]$ into internal direct sum of ideals generated by orthogonal idempotents and external direct sum of primary rings, namely, finite fields or local rings are presented. It is noted that, in contrast to finite fields, all the $P_p^n[W(a)]$ of the same order need not be isomorphic to each other. Using the decomposition of $P_p^n[W(a)]$, isomorphisms between $P_p^n[W(a)]$ of the same

order are established. An expression for the number of non-isomorphic $P_p^n[W(a)]$ of any given order is obtained in terms of number of irreducible polynomials of degree $\leq n$ and partition and restricted partition functions of integers $\leq n$.

Construction procedures for other rings isomorphic to residue class polynomial rings have been given. These are ring $Z_p^n[W]$ of n -tuples and ring $M_p^n[W]$ of $n \times n$ commutative matrices isomorphic to $P_p^n[W(a)]$ and tensor product of rings $\bigotimes^T \{Z_p^{n_i}[W_i]\}$ and $\bigotimes^T \{M_p^{n_i}[W_i]\}$ of n -tuples and $n \times n$ commutative matrices respectively, isomorphic to the tensor product $\bigotimes^T \{P_p^{n_i}[W_i(a_i)]\}$ of $P_p^{n_i}[W_i(a_i)]$; $i = 0, 1, \dots, r-1$.

Using the isomorphism between $P_p^n[W(a)]$ and $Z_p^n[W]$, it is shown that K th order $P_p^n[W(a)]$ -LSS can be implemented as K th order $Z_p^n[W]$ -LSS which constitute a subclass of $GF(p)$ -LSS of order nK and process n -tuples from $GF(p)$. These $GF(p)$ -LSS of order nK can be analysed in terms of K th order $P_p^n[W(a)]$ -LSS. This reduces analysis complexity. When $Z_p^n[W]$ is isomorphic to $P_p^n[a^n-1]$, $Z_p^n[W]$ -LSS can be obtained with serial implementation of multiplication operation using cyclic shift registers. This reduces the hardware complexity as compared to the serial operation of multiplication over $GF(p^n)$.

The decomposition of $P_p^n[W(a)]$ leads to the decomposition of $P_p^n[W(a)]$ -LSS. Thus analysis or implementation of $P_p^n[W(a)]$ -LSS can be carried out in terms of subsystems which are components of $P_p^n[W(a)]$ -LSS.

The characteristic matrix A plays a prominent role in the classification of $P_p^n[W(a)]$ -LSS and the study of periodicity properties of response of $P_p^n[W(a)]$ -LSS. Depending on whether A is nonsingular, singular or nilpotent, a $P_p^n[W(a)]$ -LSS is called nonsingular, singular or nilpotent respectively. Conditions for A to be nonsingular, singular or nilpotent are derived in terms of the nature of the coefficients of the characteristic polynomial $F(x)$ of A . It is shown that A is nonsingular (respectively singular) if a_K is a unit (respectively zero divisor) in $P_p^n[W(a)]$. A is nilpotent if the coefficients a_i ; $i = 1, 2, \dots, K$ are nilpotent in $P_p^n[W(a)]$. A bound on the index of nilpotence of A is obtained in terms of the bounds on the index of nilpotence of the coefficients a_i ; $i = 1, 2, \dots, K$, using the decomposition of $P_p^n[W(a)]$, the period T of A is shown to be equal to the lcm of the periods of the direct sum components of A .

When A is nonsingular and is of period T , it is shown that for a periodic input sequence of period J , the output sequence of $P_p^n[W(a)]$ -LSS is also periodic, whose period divides pJT .

The set of all autonomous state responses is shown to constitute a $P_p^n[W(a)]$ -module. The number of state cycles in $P_p^n[W(a)]$ -LSS is at least equal to the number of proper ideals in $P_p^n[W(a)]$. Further the period of state cycles divides the period T of A . For the sake of comparison of $P_p^n[W(a)]$ -LSS, the

ratio $T/(p^{nK}-1)$ of period T of A to the number of nonzero states, called the Figure of merit F of $P_p^n[W(a)]$ -LSS, is defined. It is shown that when $W(a)$ is irreducible over $GF(p)$, $F_{\max} = 1$. Using the decomposition of $P_p^n[W(a)]$ -LSS, the cycle length decomposition Σ of states of $P_p^n[W(a)]$ -LSS is obtained in terms of the cycle length decomposition $\Sigma_1, \Sigma_2, \dots, \Sigma_r$ of the component subsystems.

The autonomous response is a linear transformation of state response and the properties of state response carry over to autonomous response. When A is nonsingular, the autonomous response of $P_p^n[W(a)]$ -LSS is periodic irrespective of initial state. When A is singular, the autonomous response is periodic or ultimately periodic depending on the initial state. When A is nilpotent, the autonomous response is ultimately a zero sequence irrespective of the initial state.

The autonomous response of single output K th order canonical $P_p^n[W(a)]$ -LSS is a linear recursion sequence; the set of all such sequences constitutes a free $P_p^n[W(a)]$ -module of rank K . The Hamming correlation properties of such sequences of length T are studied. Using the state diagram, bounds on the Hamming correlation values are obtained. For the specific case when the ring is semisimple and the projection of characteristic polynomial of A over $W_1(a)$ is primitive over $P_p^{n_1}[W_1(a)]$ an expression for the maximum off peak normalised HACR function value and HCCR function value of sequences is obtained.

Using the concept of decompositions of ring $P_p^n[W(a)]$, it is shown that any arbitrary sequence over $P_p^n[W(a)]$ can be decomposed into sequences over orthogonal ideals in $P_p^n[W(a)]$. Such ideals have the property that two elements from distinct ideals mutually annihilate. Thus the set of decomposed sequences are elementwise orthogonal. Using the results on ring embeddings, it is shown that a sequence over primary ring or semisimple ring or semilocal ring can be transformed into a set of orthogonal sequences over a larger ring.

It is shown that sequences over orthogonal ideals can be utilised for modulation and multiplexing of data sequences in a manner analogous to spread spectrum modulation using pseudo-noise binary sequences. In a multiple access spread spectrum system, because of finite integration time in the detector, the spread spectrum carriers corresponding to undesired data streams are not completely averaged out, resulting in cross talk. This problem is not present in modulation and multiplexing based on orthogonal sequences discussed in this thesis, because the elements of the orthogonal sequences over different orthogonal ideals mutually annihilate.

Linear block codes over $P_p^n[W(a)]$ in general and linear polynomial and linear cyclic codes over $P_p^n[W(a)]$ in particular have been studied and possibilities of encoding and decoding of linear polynomial and cyclic codes over $P_p^n[W(a)]$ using

$P_p^n[W(a)]$ -LSS are explored. It is shown that in the specific case of codes over $Z_2^n[W] \simeq P_2^n[a^n-1]$, use of cyclic shift registers for implementing multiplication, reduces the hardware complexity of encoders.

6.2 SUGGESTIONS FOR FURTHER WORK

We have presented a comprehensive theory for $P_p^n[W(a)]$ -LSS and considered their applications to generation of sequences and encoding and decoding polynomial and cyclic codes. While some of the basic issues such as implementation and analysis of $P_p^n[W(a)]$ -LSS have been reasonably settled, this study has opened new areas for further investigations. In particular investigations in the following directions may be taken up.

(i) It is shown here that $P_p^n[W(a)]$ can be decomposed into internal direct sum of ideals generated by orthogonal idempotents or external direct sum of primary rings which are either finite fields or local rings. This leads to the notion of decomposition of systems. Using this result expressions for period of characteristic matrix A , and cycle length decomposition Σ of states of $P_p^n[W(a)]$ -LSS are obtained in terms of the corresponding quantities of component subsystems. Thus $P_p^n[W(a)]$ -LSS are analysed in terms of component subsystems over finite field or local rings. In this thesis Σ of systems over local $P_p^n[W(a)]$ are obtained in terms of Σ of isomorphic

$GF(p)$ -LSS. It is worthwhile to study local $P_p^n[W(a)]$ -LSS on their own, in which case analysis of $P_p^n[W(a)]$ -LSS can be done purely in terms of its component subsystems.

(ii) For the sake of comparison of various autonomous K th order $P_p^n[W(a)]$ -LSS from the point of view of their capability to generate periodic sequences, a figure of merit F is defined. It is the ratio of maximum possible length T of the sequence generated and the number $(p^{nK}-1)$ of nonzero states in $P_p^n[W(a)]$ -LSS. The sequence generators which generate maximum length sequence over $GF(p^n)$ have $F = 1$, the maximum possible value. It will be worthwhile to investigate the maximum possible value of F for generators over various $P_p^n[W(a)]$ -LSS.

(iii) Modulation and multiplexing of data sequences in a manner analogous to spread spectrum modulation is given as an application of sequences over orthogonal ideals. It is also pointed out that in a multiple access spread system because of finite integration time in the detector the spread spectrum carriers corresponding to undesired data streams are not completely averaged out, resulting in cross talk. This problem is not present in the scheme employing sequences over orthogonal ideals. However, the noise performance of modulation and multiplexing scheme proposed in this thesis needs investigation.

(iv) The theory of linear block codes and polynomial and cyclic codes over $P_p^n[W(a)]$ developed in this thesis is from the point of view of application of $P_p^n[W(a)]$ -LSS in the encoding and decoding of these codes. Investigation is needed to study the performance and to see whether good codes exist over $P_p^n[W(a)]$ rings compared to codes over finite fields. In the permutation decoding of cyclic codes over $P_p^n[W(a)]$ discussed in the thesis, only certain patterns of t errors in which there is a spacing of at least K symbols between any two such error locations, are corrected. Permutation decoding which corrects all patterns of t -errors needs further study. Besides this, convolutional codes over $P_p^n[W(a)]$ need investigation.

(v) The analysis of autonomous $P_p^n[W(a)]$ -LSS has been carried out in detail in this thesis. Synthesis aspects of $P_p^n[W(a)]$ -LSS constitute a good topic for study.

(vi) In this thesis study of autonomous response and some applications of $P_p^n[W(a)]$ -LSS are carried out. It is worthwhile to study the response and applications of $\bigotimes^T \{P_p^{n_i}[W_i(a)]\}$ -LSS. The operational calculus techniques for LSS over residue class integer rings are given in [43]. Counterpart of these techniques for $P_p^n[W(a)]$ -LSS needs investigation.

(vii) It is seen that the response of a nonsingular $P_p^n[W(a)]$ -LSS is periodic if input is periodic. With appropriate constraints on the system the output period may be made greater than the input period and hence $P_p^n[W(a)]$ -LSS may be used as a data scrambler in a manner similar to data scramblers over finite fields [30,31]. Investigations of various aspects of $P_p^n[W(a)]$ data scramblers thus constitute another good topic for further investigation.

APPENDIX A

NUMBER OF IRREDUCIBLE POLYNOMIALS OF A GIVEN DEGREE OVER FINITE FIELD OF ORDER q

The number η_i of irreducible polynomials of degree i over a finite field of order q [18] is given by

$$\eta_i = \frac{1}{i} \sum_{\substack{d \\ d|i}} \mu(d) q^{i/d} \quad (\text{A.1})$$

where $\mu(d)$ is the Mobius function

$$\mu(d) = 1 \text{ for } d=1$$

$$= (-1)^k, \text{ where } d \text{ is the product of } k \text{ distinct prime factors}$$

$$= 0, \text{ where } d \text{ is the product of repeated prime factors}$$

Summation is over all d 's which divide i including $d=1$ and i .

Example A.1:

Number of irreducible polynomials of degree 4 over
GF(2)

$$\begin{aligned} \eta_4 &= \frac{1}{4} \sum_{\substack{d \\ d|4}} \mu(d) 2^{4/d} \\ &= \frac{1}{4} [\mu(1)2^4 + \mu(2)2^2 + \mu(4)2] \\ &= \frac{1}{4} [2^4 - 2^2] = 3 \end{aligned}$$

Example A.2:

Number of irreducible polynomials of degree 5
over GF(3) .

$$\begin{aligned}
 \eta_5 &= \frac{1}{5} \sum_{\substack{d \\ d|5}} \mu(d) 3^{5/d} \\
 &= \frac{1}{5} [\mu(1) 3^5 + \mu(5) 3] \\
 &= \frac{1}{5} [243 - 3] = 48
 \end{aligned}$$

APPENDIX B

MIXED RADIX NUMBER SYSTEM

Here we discuss the representation of numbers with respect to a set of mixed radices.

Decimal and binary number systems are examples of fixed radix number systems.

For example decimal $567 = 5 \times 10^2 + 6 \times 10 + 7 \times 10^0$
and binary $1101 = 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$,

where the fixed radices are 10 and 2 respectively.

Numbers can also be represented with respect to a set of mixed radices. Consider a set of numbers,

$$\{0, 1, \dots, n-1\} \quad (B.1)$$

and another set of numbers $\{n_0, n_1, \dots, n_{r-1}\}$, called mixed

radices, where $n_i > 1$ and $\prod_{j=0}^{r-1} n_j = n$.

Defining $\omega_j = \prod_{K=0}^{j-1} n_K$ and $\omega_0 = 1$,

any number i belonging to the set (B.1) can then be represented with respect to the mixed radices $\{n_0, \dots, n_{r-1}\}$ as

$$i = i_{r-1}\omega_{r-1} + i_{r-2}\omega_{r-2} + \dots + i_j\omega_j + \dots + i_1\omega_1 + i_0\omega_0$$

$$\langle i_{r-1}, i_{r-2}, \dots, i_1, i_0 \rangle$$

we note that in decimal and binary number systems w_i 's are powers of 10 and 2 respectively.

In mixed radix number system w_i 's are product of numbers and are called the weights of the mixed radix number system, i_j are mixed radix digits the constraints on i_j is $0 \leq i_j < n_j$.

Example B.1:

Consider the set of numbers $\{0, 1, 2, 3, 4, 5\}$. Here $n = 6 = 3 \times 2$. Taking $n_0 = 3$ and $n_1 = 2$, the representation of numbers from 0 to 5 with respect to the mixed radices 3 and 2 are given in Example 2.6.7, where $w_0=1$, $w_1=n_0=3$. If we take $n_0=2$ and $n_1=3$, we get another representation which is given below. Here $w_0=1$, $w_1=n_0=2$

i	0	1	2	3	4	5
$\langle i_1 i_0 \rangle$	$\langle 00 \rangle$	$\langle 01 \rangle$	$\langle 10 \rangle$	$\langle 11 \rangle$	$\langle 20 \rangle$	$\langle 21 \rangle$

APPENDIX C

PROPERTIES OF KRONECKER PRODUCT OF MATRICES

Some relevant properties of Kronecker product of matrices [57-59, 61] are given here.

Let

$$A = \begin{bmatrix} a_{00} & a_{01} & \dots & a_{0\ n-1} \\ a_{10} & a_{11} & \dots & a_{1\ n-1} \\ a_{n-10} & a_{n-11} & \dots & a_{n-1\ n-1} \end{bmatrix}$$

$$B = \begin{bmatrix} b_{00} & b_{01} & \dots & b_{0\ m-1} \\ b_{10} & b_{11} & \dots & b_{1\ m-1} \\ b_{m-10} & b_{m-11} & \dots & b_{m-1,\ m-1} \end{bmatrix}$$

Then the Kronecker product of matrices A and B is defined as

$$A \otimes B = \begin{bmatrix} a_{00}B & a_{01}B & \dots & a_{0\ n-1}B \\ a_{10}B & a_{11}B & \dots & a_{1\ n-1}B \\ a_{n-1,0}B & a_{n-1,1}B & \dots & a_{n-1\ n-1}B \end{bmatrix}$$

Let $C = A \otimes B$

Then ij th element of C is given by

$$C_{ij} = C_{\langle i_1 i_0 \rangle \langle j_1 j_0 \rangle} = a_{i_1 j_1} b_{i_0 j_0},$$

where $\langle i_1 i_0 \rangle$ is the mixed radix number system representation of i with respect to mixed radices n, m respectively.

Example C.1:

Consider

$$A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} ; B = \begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix}$$

Here $n=2$; $m=3$

Let $C = A \otimes B$ C is a 6×6 matrix

The element C_{35} in C is found as follows. The mixed radix number representation of 3 and 5 with respect to mixed radices $n=2$ and $m=3$ are $\langle 10 \rangle$ and $\langle 12 \rangle$ respectively.

Here $C_{35} = C_{\langle 10 \rangle \langle 12 \rangle} = a_{11} b_{02}$, which is verified below.

$$C = \begin{bmatrix} a_{00} b_{00} & a_{00} b_{01} & a_{00} b_{02} & a_{01} b_{00} & a_{01} b_{01} & a_{01} b_{02} \\ a_{00} b_{10} & a_{00} b_{11} & a_{00} b_{12} & a_{01} b_{10} & a_{01} b_{11} & a_{01} b_{12} \\ a_{00} b_{20} & a_{00} b_{21} & a_{00} b_{22} & a_{01} b_{20} & a_{01} b_{21} & a_{01} b_{22} \\ a_{10} b_{00} & a_{10} b_{01} & a_{10} b_{02} & a_{11} b_{00} & a_{11} b_{01} & a_{11} b_{02} \\ a_{10} b_{10} & a_{10} b_{11} & a_{10} b_{12} & a_{11} b_{10} & a_{11} b_{11} & a_{11} b_{12} \\ a_{10} b_{20} & a_{10} b_{21} & a_{10} b_{22} & a_{11} b_{20} & a_{11} b_{21} & a_{11} b_{22} \end{bmatrix}$$

The properties of Kronecker product of matrices are listed below.

1. $A \otimes \underline{0} = \underline{0} \otimes B = \underline{0}$
2. $I_{n \times n} \otimes I_{m \times m} = I_{mn \times mn}$
3. $(A_1 + A_2) \otimes B = (A_1 \otimes B) + (A_2 \otimes B)$
4. $A \otimes (B_1 + B_2) = (A \otimes B_1) + (A \otimes B_2)$
5. $\alpha A \otimes \beta B = \alpha\beta(A \otimes B)$; α, β scalars
6. $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$
7. $(A_1 \otimes B_1)(A_2 \otimes B_2) = A_1 A_2 \otimes B_1 B_2$
8. $(A \otimes B) = (A \otimes I)(I \otimes B) = (I \otimes B)(A \otimes I)$.

APPENDIX D

PROCEDURE FOR DETERMINATION OF ELEMENTARY DIVISORS OF MATRICES
AND COMPUTATION OF PERIOD OF POLYNOMIALS OVER FINITE FIELDS

In this appendix, procedure for computing elementary divisors of $K \times K$ square matrix A and the computation of period of polynomials over finite fields are summarised.

Given A , consider the matrix $A(x) = (xI - A)$. The principal diagonal of this matrix contains first degree polynomials, all off diagonal elements are zero degree polynomials or zeroes. This is a special case of polynomial matrices.

The following three operations called elementary row (column) operations can be performed on $A(x)$.

- i) interchange of any two rows (columns)
- ii) multiplication of a row (column) by a nonzero element of field
- iii) addition of any row(column) multiplied by a polynomial to another row (column).

Two matrices $A(x)$ and $B(x)$ are said to be equivalent, if $A(x)$ can be carried to $B(x)$ by means of finite number of elementary operations. Given matrix $A(x)$ an equivalent matrix, in canonical form is obtained by finite number of elementary operations. The canonical matrix has the following properties:

i) the matrix is diagonal, that is, it is of the form

$$A_c(x) = \begin{bmatrix} d_1(x) & & & \\ & d_2(x) & & \\ & & \ddots & \\ & & & d_K(x) \end{bmatrix} \quad (D.1)$$

ii) any polynomial $d_i(x)$, $i=1,2,\dots,K$ is divisible by the polynomial $d_{i-1}(x)$

iii) every nonzero polynomial $d_i(x)$; $i=1,2,\dots,K$ is monic
 $A_c(x)$ is called Smith's canonical form of $A(x)$.

Any matrix $A(x)$ can be reduced to Smith's canonical form via elementary operations.

Let $\Theta_r(x)$ denote the gcd of all the r th order minors of $A(x)$; $1 \leq r \leq K$. We thus have the polynomials

$$\Theta_1(x), \Theta_2(x), \dots, \Theta_K(x) \quad (D.2)$$

which are uniquely defined by the matrix $A(x)$, and remains unchanged under elementary operations, $\Theta_1(x)$ is the gcd of all elements of $A(x)$, and $\Theta_K(x)$ is equal to the determinant of the matrix $A(x)$ divided by its leading coefficient.

The matrix,

$$A_{rc} = \begin{bmatrix} M_{11} & & & & \\ & M_{1r} & & & \\ & & M_{21} & & \\ & & & \ddots & \\ & & & & M_{2r} \\ & & & & & \ddots \\ & & & & & & M_{K1} \\ & & & & & & & \ddots \\ & & & & & & & & M_{Kr} \end{bmatrix}$$

where M_{ij} is the companion matrix of $[\lambda_j(x)]^{h_{ij}}$, is called the rational canonical form of A . A and A_{rc} are similar.

We now consider the determination of period of polynomials over finite field $GF(p^n)$.

Suppose $f(x)$ is an irreducible polynomial of degree K over $GF(p^n)$. Let α be a root of $f(x)$ over $GF(p^{nK})$. The least integer j , such that $\alpha^j = 1 \pmod{[p, f(\alpha)]}$ is called the multiplicative order of α . In general, $j \mid (p^{nK} - 1)$. If $j = (p^{nK} - 1)$, then α is called a primitive element in $GF(p^{nK})$ and $f(x)$ is called a primitive polynomial over $GF(p^n)$. If α is primitive, then the powers of α , that is,

$\{\alpha, \alpha^2, \alpha^3, \dots, \alpha^{p^{nK}-1}\}$, are the nonzero field elements.

Given a polynomial $g(x)$ over $GF(p^n)$, the smallest integer e for which $g(x) \mid (x^e - 1)$, is called the exponent or

period of $g(x)$. If $g(x)$ is an irreducible polynomial of degree K over $GF(p^n)$, then the period of $g(x)$ is equal to the multiplicative order of its roots which is a factor of $(p^{nK}-1)$.

Suppose $g(x)$ of degree K is irreducible over $GF(p^n)$. Let its period be e . Then period of $g^h(x)$ is given by $p^r e$, where p^r is such that, $p^{r-1} < h \leq p^r$. If $g(x) = g_1^{h_1}(x) \cdot g_2^{h_2}(x) \dots g_y^{h_y}(x)$. Where $g_i(x)$ are irreducible polynomials over $GF(p^n)$, then period of $g(x)$ is the least common multiple of periods of $g_1^{h_1}(x) g_2^{h_2}(x) \dots g_y^{h_y}(x)$.

Example D.1:

Consider the polynomial

$$g(x) = (x^2 + \alpha x + \alpha)^3 (x + \alpha)^3 \text{ over } GF(2^2) = \{0, 1, \alpha, \alpha^2\};$$

$$\alpha^2 + \alpha + 1 = 0 \text{ and } \alpha^3 = 1.$$

$g_1(x) = (x^2 + \alpha x + \alpha)$ is irreducible over $GF(2^2)$. Let β be a root of $g_1(x)$ then $\beta^2 + \alpha\beta + \alpha = 0$. We see that

$$\beta^{15} = 1 \pmod{[2; g(\beta)]}.$$

multiplicative order of β is 15 and hence period of $g_1(x)$ is 15.

Period of $g_1^3(x)$ is $2^2 \times 15 = 60$, since $2^1 < 3 < 2^2$.

Similarly, we have $g_2(x) = (x + \alpha)$

$$\text{and } \beta^3 = 1 \pmod{[2; g_2(\beta)]}$$

Hence period of $g_2(x)$ is 3.

Period of $g_2^3(x)$ is $2^2 \times 3 = 12$ since $2^1 < 3 \leq 2^2$.

Period of $(x^2+ax+\alpha)^3(x+\alpha)^3 = \text{lcm}[60, 12] = 60$.

Period of $g(x)$ can also be determined without factorisation, when $g(x)$ is of small degree. By definition, period of $g(x)$ is the least integer e such that $g(x) \mid (x^e - 1)$, that is, least integer e such that $x^e = 1$ modulo $[p; g(x)]$.

APPENDIX E

CHINEESE REMAINDER THEOREM

The Chinese Remainder Theorem for integer and polynomials [18] is given below.

- i) For integers: Given primes p_1, p_2, \dots, p_k and integers c_1, c_2, \dots, c_k the simultaneous congruences

$$c = c_i \text{ modulo } p_i^{e_i} \quad i = 1, 2, \dots, k \text{ have a unique}$$

$$\text{solution modulo } \prod_{i=1}^k p_i^{e_i}$$

- ii) For polynomials: Given irreducible polynomials $W_1(a), W_2(a) \dots W_k(a)$ and arbitrary polynomials $r_1(a), \dots, r_k(a)$ over a finite field $GF(p)$, the simultaneous congruences

$$r(a) = r_i(a) \text{ modulo } [p; W_i^{h_i}(a)] \text{ have a unique}$$

$$\text{solution for } r(a) \text{ modulo } \prod_{i=1}^k W_i^{h_i}(a).$$

Proof: (For polynomials).

Since $\overline{h_i} = \prod_{j \neq i}^k W_j^{h_j}(a)$ has no factors in common with $W_i^{h_i}(a)$, we may use Euclid's algorithm to find a polynomial $b_i(a)$ such that

$b_i(a) \prod_{j \neq i}^k W_j^{h_j}(a) = 1 \text{ modulo } W_i^{h_i}(a)$, then setting

$$r(a) = \sum_{i=1}^k r_i(a) b_i(a) \prod_{j \neq i}^k W_j^{h_j}(a)$$

It is seen that,

$$r(a) = r_i(a) \text{ modulo } W_i^{h_i}(a) \text{ for all } i.$$

If $r'(a)$ also solves these simultaneous congruences then $r(a) - r'(a)$ is divisible by $W_i^{h_i}(a)$ for $i=1, 2, \dots, k$.

So $r'(a) = r(a) \text{ modulo } \prod_{i=1}^k W_i^{h_i}(a)$.

The theorem for the case of integers can be proved analogously.

APPENDIX F

NUMBER OF UNITS IN $P_p^n[W(a)]$

The units in $P_p^n[W(a)]$ are the polynomials in variable a over $GF(p)$, which are relatively prime to $W(a)$. If $W(a)$ is irreducible then all nonzero elements are relatively prime to $W(a)$ and are units in $P_p^n[W(a)]$. In general, $r(a) \in P_p^n[W(a)]$ is a unit iff $(r(a), W(a)) = 1$. The number of monic polynomials $r(a)$ of degree $\leq n$ such that $(r(a), W(a)) = 1$ is given by the Euler function for the polynomials over $GF(p)$, given by the formula [83].

$$\phi(W(a)) = p^n \prod_{r(a) | W(a)} \left[1 - \frac{1}{|r(a)|} \right].$$

where $r(a)$ runs through all monic prime divisors of $W(a)$ and $|r(a)| = p^{n_r}$, where n_r is the degree of $r(a)$. The number of units in $P_p^n[W(a)]$ is hence $(p-1) \cdot \phi(W(a))$.

APPENDIX G

POLYNOMIAL CODES OVER $GF(p^n)$

The general theory of polynomial codes defined by polynomials in one variable is given in [84], a special case of which is the Reed Solomon Code. This code is a mapping of a vector space of dimension K with basis $1, x, x^2, \dots, x^{K-1}$ into a vector space of dimension N with a set of N Lagrangians $L_1(x), L_2(x), \dots, L_N(x)$ as the basis where

$$L_i(x) = \prod_{j=1}^N \frac{(x - \alpha_j)}{(\alpha_i - \alpha_j)} \quad i = 1, 2, \dots, N.$$

and $\alpha_1, \alpha_2, \dots, \alpha_N$ are the distinct elements in $GF(p^n)$.

If we call

$$F(x) = \sum_{i=0}^{K-1} u_i x^i \quad \text{as the message polynomial}$$

the corresponding code polynomial is $\sum_{i=1}^N F(\alpha_i) L_i(x)$.

In other words it is a mapping of the K -tuples

$(u_0, u_1, \dots, u_{K-1})$ to an N -tuple

$$(F(\alpha_1), F(\alpha_2), \dots, F(\alpha_N))$$

Such a formulation of polynomial codes over $P_p^n[W(a)]$ in general is not possible, for in the computation of Lagrangians, in the denominator, the difference of two elements from $P_p^n[W(a)]$, may lead to a zero divisor.

APPENDIX H

COMPARISON OF $P_p^n[W(a)]$ and Z_m

Though $P_p^n[W(a)]$ and Z_m are finite commutative rings there are certain similarities and dissimilarities in these two rings. As a consequence the properties, analysis and implementation of linear sequential systems LSS over $P_p^n[W(a)]$ and Z_m will be different. The similarities and dissimilarities of these two rings and LSS over these rings are summarised.

Similarities in $P_p^n[W(a)]$ and Z_m :

1. The role of irreducible polynomial and power of irreducible polynomial in $P_p^n[W(a)]$ is same as the role of prime and prime powers in Z_m . The type of $P_p^n[W(a)]$ and Z_m depend on type of $W(a)$ and Z_m respectively.

2. The notion of decomposition in the case of $P_p^n[W(a)]$ and Z_m are similar.

Dissimilarities:

1. In general Z_m is not isomorphic to $P_p^n[W(a)]$. However when $m=p$ a prime $Z_p = P_p^1[W(a)] = GF(p)$.

2. $P_p^n[W(a)]$ has the structure of both a commutative ring and a vector space. Hence $P_p^n[W(a)]$ is a commutative algebra.

Ring of n -tuples and $n \times n$ commutative matrices over $GF(p)$, isomorphic to $P_p^n[W(a)]$ can be constructed. Z_m is a module over itself of rank 1.

3. For any m there is a residue class ring Z_m of integers modulo m which is of order m . However the order of $P_p^n[W(a)]$ is of the form p^n . When n is a prime the polynomials in the residue class polynomial ring, are in single variable. When n is composite in addition to residue class ring of polynomials in one variable, there is tensor product of residue class polynomial rings. The tensor product ring is isomorphic to finite commutative ring of polynomials in more than one variable.

4. When $m=p^n$ there is only one residue class ring of integers Z_m . There is more than one nonisomorphic residue class polynomial rings of order p^n ; in addition, when n is composite we have many nonisomorphic tensor product of residue class polynomial rings of order p^n .

5. It is possible that a semisimple ring $P_p^n[W(a)]$ is isomorphic to the external direct sum of ν Galois fields of the same order. The number ν depends on the number of irreducible polynomials of a given degree, over $GF(p)$.

If Z_m is semisimple it is isomorphic to the external direct sum of finite fields of different order.

In the implementation and analysis of $P_p^n[W(a)]$ -LSS and Z_m -LSS the following differences arise.

$P_p^n[W(a)]$ -LSS	Z_m -LSS
1. Memory device store element of $P_p^n[W(a)]$ or n-tuple over $GF(p)$.	1. Memory device store element of Z_m .
2. Analysis of $GF(p)$ -LSS $\simeq P_p^n[W(a)]$ -LSS can be done in terms of $P_p^n[W(a)]$ -LSS.	2. Z_m -LSS is not isomorphic to any $GF(p)$ -LSS unless $m=p$.

The procedures in the computation of period of characteristic matrix A of LSS over $P_p^n[W(a)]$ and LSS over Z_m are same. The procedure for the enumeration of state cycles of $P_p^n[W(a)]$ -LSS and Z_m -LSS are same. However when $P_p^n[W(a)]$ is a local ring the analysis of $P_p^n[W(a)]$ -LSS can be done in terms of the isomorphic $GF(p)$ -LSS. The isomorphism between $P_p^n[W(a)]$ -LSS and $GF(p)$ -LSS is also used in the implementation of $P_p^n[W(a)]$ -LSS.

REFERENCES

1. Gill, A., 'Introduction to the Theory of Finite-State Machines', McGraw-Hill, New York, 1962.
2. Hennie, F.C., 'Finite-state Models for Logical Machines,' Wiley, New York, 1968.
3. Huffman, D.A., 'The Synthesis of Linear Sequential Coding Networks', in 'Linear Sequential Switching Circuits' (W.H. Kautz ed.), Holdenday San Fransisco, California 1965.
4. Elspas, B., 'The Theory of Autonomous Linear Sequential Networks', IRE Trans. CT-6, pp. 45-60, Mar. 1959.
5. Hartmanis, J., 'Linear Multivalued Sequential Coding Networks', IRE Trans., CT-6, pp. 69-74, Mar. 1959.
6. Friedland, B., 'Linear Modular Sequential Circuits', IRE Trans. CT-6, pp. 61-68, Mar. 1959.
7. Friedland, B. and Stern, T.E., 'On Periodicity of States in Linear Modular Sequential Circuits', IRE Trans., IT-5, pp. 136-137, Sept. 1959.
8. Stern, T.E. and Friedland, B., 'The Linear Modular Sequential Circuit Generalised', IRE Trans. CT-8, pp. 79-80, 1961.
9. Zierler, N., 'Several Binary Sequence Generators', In Linear Sequential Switching Circuits (W.H. Kautz ed.) Hodenday San Fransisco, California 1965.
10. Zierler, N., 'Linear Recurring Sequences', J. Soc. Indust. Appl. Math., vol. 7, pp. 31-48, Mar. 1959.
11. Golomb, S.W., 'Shift Register Sequences', San Fransisco, Holdenday Inc. 1967.
12. Gill, A., 'Linear Sequential Circuits Analysis and Applications', McGraw-Hill Book Co., New York, 1967.
13. Gill, A., in 'System Theory' Ed. Zadeh L.A. and Polak, E., Tata McGraw Hill Publishing Co. Ltd. New Delhi 1969.

14. Booth, T.L., 'Sequential Machines and Automata Theory', Wiley, New York, 1967.
15. Kautz, W.H. (ed.), 'Linear Sequential Switching Circuits', Selected Technical Papers, Holden-day, Inc., Sanfransisco, 1965.
16. David Forney, D., 'Convolutional Codes I: Algebraic Structure, IEEE Trans. Inf. Theory, vol. IT-16, pp. 720-738, Nov. 1976.
17. Massey, J.L., 'Applications of Automata Theory in Coding', In Applied Automata Theory, Academic Press Inc., New York, 1968.
18. Berlekamp, E.R., 'Algebraic Coding Theory', McGraw Hill, Book Co., New York, 1968.
19. Peterson, W.W. and Weldon, E.J. Jr., 'Error Correcting Codes, 2nd Ed. Cambridge, MIT, 1972.
20. MacWilliams, F.J. and Sloane, N.J.A., 'The Theory of Error Correcting Codes', North Holland Pub. Co. 1977.
21. Lin, S. and Costello, D.J. Jr., 'Error Control Coding Fundamentals and Applications', Prentice Hall, Inc. Englewood Cliffs, New Jersey, 1983.
22. Lempel, A., and Greenberger, H., 'Families of Sequences with Optimal Hamming correlation properties', IEEE Trans. Inf. Theory, IT-20, pp. 90-94, Jan. 1974.
23. Balza, C., Fromageot, A., and Maniere, M., 'Four Level Pseudorandom Sequences, Electronics Letters, vol. 3, pp. 313-315, July, 1967.
24. Brigg, P.A.N. and Godfrey, K.R., 'Autocorrelation Function of a Four Level m-1 Sequence', Electronics Letters, pp. 232-283, May, 1968.
25. Carmichael, R.D., 'On Sequences of Integers Defined by Recurrence Relations', Quarterly J. of Math. 48, pp. 343-372, 1920.
26. Ward, M., 'The Arithmetical Theory of Linear Recurring Series', Trans. Am. Math. Soc., vol. 35, pp. 600-628, 1933.

27. Hall, M., 'An Isomorphism Between Linear Recurring Sequences and Algebraic Rings', Trans. Am. Math. Soc., vol. 44, pp. 196-218, 1938.
28. MacWilliams, F.J. and Sloane, N.J.A., 'Pseudo random Sequences and Arrays', Proc. IEEE, vol. 64, pp. 1715-1729, Dec. 1976.
29. Sarwate, D.V. and Pursley, A.M.B., 'Cross-correlation Properties of Pseudorandom and Related Sequences', Proc. IEEE, vol. 68, pp. 593-619, May 1980.
30. Savage, J.E., 'Some Simple Self-synchronising Digital Data Scramblers', Bell Syst. Tech. J. 46, pp. 449-487, Feb. 1967.
31. Nakamura, K. and Iwadare, Y., 'Data Scramblers for Multilevel Pulse Sequences', Electronics and Communications in Japan, vol. 55-A, No. 6, pp. 8-16, June 1972.
32. Dixon, R.C., 'Spread Spectrum Systems', New York, Wiley 1975.
33. Dixon, R.C. Ed. 'Spread Spectrum Technique', IEEE Press, 1976.
34. Holmes, J., 'Coherent Spread Spectrum Systems', Wiley Interscience, John Wiley and Sons, 1982.
35. Gold, R., 'Optimal Binary Sequences for Spread Spectrum Multiplexing', IEEE Trans. Inf. Theory, IT-13, pp. 619-621, Oct. 1967.
36. Sergio, J.R. and Hayes, J.F., 'Analysis and Simulation of a PN Synchronisation System', IEEE Trans. Commn. Tech., COM-18, pp. 676-679, Oct. 1970.
37. Price, R. and Green, P.E. Jr., 'A Communication Technique for Multipath Channels', Proc. IRE, vol. 46, pp. 555-570, Mar. 1958.
38. David, R. and Blanchet, G., 'About Random Fault Detection in Combinational Networks', IEEE Trans. on Computer', C-25, pp. 659-664, June 1976.

39. Painter, J.H., 'Designing Pseudorandom coded Ranging System', IEEE Trans. on Aerospace and Electronic Systems, Jan. 1967.
40. Bollman, D.A., 'Some Periodicity Properties of Transformations on Vector Spaces over Residue Class Rings', J. Soc. Indust. Appl. Math., vol. 13, pp. 902-912, Sept. 1965.
41. Bollman, D.A., 'Some Periodicity Properties of Modules over the Ring of Polynomials with Coefficients in a Residue Class Ring', J. SIAM App. Math., vol. 14, pp. 237-241, Mar. 1966.
42. Matluk, M.M. and Gill, A., 'Linear Sequential Circuits over Rings', Proc. Int. IEEE Conf. on Systems, Networks and Computers, vol. I, 1971.
43. Richalet, J., 'Operational Calculus for Finite Rings', IEEE Trans. Circuit Theory, CT-12, pp. 558-562, Dec. 1965.
44. Sontag, E.D., 'Linear Systems over Commutative Rings: a Survey', Ricerche DI Automatica, vol. 7, No. 1 July 1976, pp. 1-33.
45. Sontag, E.D., 'Linear Systems over Commutative Rings: A (partial) Updated Survey', Mathematical System Theory III, IFAC Control Science and Technology, (8th Triennial World Congress), Kyoto, Japan, pp. 325-330, 1981.
46. Rouchaleau, Y., 'Linear Discrete Time Finite Dimensional Dynamical Systems over some Classes of Commutative Rings', Ph.D. Dissertation, Stanford, 1972.
47. Rouchaleau, Y., Wyman, B.F., and Kalman, R.E., 'Algebraic Structure of Linear Dynamical Systems. III Realisation Theory over a Commutative Ring, Proc. Nat. Acad. Sci. USA, vol. 69, No. 11, pp. 3404-3406, Nov. 1972.
48. Blake, I.F., 'Codes over Certain Rings', Inf. Cont., vol. 20, pp. 396-404, May 1972.
49. Blake, I.F., 'Codes over Integer Residue Rings', Inf. Cont., vol. 29, pp. 295-300, Dec., 1975.

50. Spiegel, E., 'Codes over Z_m ', Inf. and Cont., vol. 35, pp. 48-51, Sept. 1977.
51. Murakami, H. and Reed, I.S., 'Multichannel Convolutional Coding Systems over a Direct Sum of Galois Fields', IEEE Trans. Inf. Theory, IT-24, pp. 205-212, Mar. 1978.
52. Kader, C.M., Rabiner, L.R. and Schafer, R.W., 'A fast Method of Generating Digital Random Numbers', Bell Syst. Tech. J; 49, pp. 2303-2310, Nov. 1970.
53. Viterbi, A.J. and Omura, J.K., 'Principles of Digital Communication and Coding', McGraw Hill, Koga Kusha Ltd., 1979.
54. MacWilliams, F.J., 'Permutation Decoding of Systematic Codes', Bell. Syst. Tech. J., vol. 43, pp. 485-505, Jan. 1964.
55. Niven, I., and Zuckerman, H.S., 'An Introduction to Theory of Numbers', Third Ed., Wiley Eastern, 1972.
56. Siddiqi, M.U., 'A Study of Permutation Invariant Linear Systems', Ph.D. Thesis, EE Dept., I.I.T. Kanpur, June, 1976.
57. Gantmacher, F.R., 'The Theory of Matrices' New York, Chelsea, 1959, vol. 1.
58. MacDuffee, C.C., The Theory of Matrices Springer Berlin 1933, Reprinted by Chelsea Publishing Company, N.Y. 1950.
59. Lancaster, P., Theory of Matrices, Academic Press NY and London 1969.
60. Herstein, I.N., Topics in Algebra, Vikas Publishing House Pvt. Ltd. 1975.
61. Halmos, P.R., 'Finite Dimensional Vector Spaces', D. Van Nostrand Co., Affiliated East West Press Pvt. Ltd., New Delhi 1958.
62. Hoffman, K. and Kunze R., Linear Algebra, Prentice Hall of India 1971.

63. Hartley, B. and Hawkes, T.O., 'Rings Modules and Linear Algebra', Chapman and Hall Ltd., 1970.
64. Hollister, H.A., 'Modern Algebra, a First Course', Harper and Publishers, 1972.
65. Birkhoff, G. and Bartee, T.C., 'Modern Applied Algebra', McGraw-Hill Book Co., 1970.
66. Mostow, G.D., Sampson, J.H. and Meyer, J.P., 'Fundamental Structures of Algebra', International Student Edition, McGraw-Hill, Book Co., Kogakusha Co. Japan, 1963.
67. MacLanes and Birkhoff, G., 'Algebra' MacMillan, 1967.
68. Northcott, D.G., 'Lessons on Rings Modules and Multiplicities', Cambridge University Press, 1968.
69. Zariski, O., and Samuel P., 'Commutative Algebra', vol. I, D. Van Nostrand Company Inc., 1958.
70. Marvin Marcus, 'Introduction to Modern Algebra', Marcel Dekker Inc., 1978.
71. McCoy, N.H., 'Rings and Ideals', The Carus Mathematical Monographs, The Mathematical Association of America, 1948.
72. Atiyah, M.F. and MacDonald, I.G., 'Introduction to Commutative Algebra', Addison-Wesley Publishing Company, 1969.
73. Lang, S., 'Algebra', Addison Wesley Publishing Company, 1965.
74. Kasch, F., 'Modules and Rings', translated by D.A.R. Wallace Lond., Math. Society, Academic Press 1982.
75. Hinehart, R.F., 'Commutative Algebras which are Polynomial Algebras', Duke J. of Maths., vol. 4, pp. 725-736, 1938.
76. Kurosh, A., 'Higher Algebra', (English Translation) MIR Publishers, Moscow, 1972.

77. McCoy N.H., 'Concerning Matrices with Elements in a Commutative Ring', Bulletin of the American Math. Soc., vol. 45, pp. 280-284, 1939.
78. Scholtz, R.A., and Welch, L.R., 'GMW Sequences', IEEE Trans. Inf. Theory, vol. IT-30, No. 3, pp. 548-553, May, 1984.
79. Naimark, M., 'Normed Rings', Translated from the first Russian Edition by Leo F. Boron., Groningen P. Noordhoff, 1964.
80. Berlekamp, E.R., 'Bit Serial Reed Solomon Encoders', IEEE Trans., Inf. Theory, IT-28, pp. 869-874, Nov. 1982.
81. Tietavainen, A., On the Nonexistence of Perfect Codes over Finite Fields, SIAM J.App.Math., vol. 24, pp. 88-96, Jan. 1973.
82. Reed, I.S. and Solomon, G., 'Polynomial Codes over Certain Finite Fields', J. Soc. Ind. Appl. Math., vol. 8, pp. 300-304, June 1960.
83. Carlitz, L. and Hodges, J.H., 'Distribution of Matrices in a Finite Field', Pacific J. of Maths. vol. 6, pp. 225-230, 1956.
84. Goethals, J.M., 'A Polynomial Approach to Linear Codes', Philips Research Report, 24, pp. 145-159, 1969.